

| | | |
|-------------------------------|--|-----------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | |

Comune di Monte Argentario

Documento programmatico
sulla sicurezza dei dati

D.Lgs. 196/2003

REVISIONE MARZO 2010

| | | |
|-------------------------------|--|------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 1 di 40 |

1. Introduzione

2. Elenco dei trattamenti di dati personali

- 2.1 Dati trattati dal personale interno
- 2.2 Dati trattati il cui trattamento è affidato all'esterno

3. Distribuzione dei compiti e delle responsabilità

- 3.1 Individuazione ed attribuzioni del responsabile
- 3.2 I responsabili esterni
- 3.3 Gli incaricati
- 3.4 L'amministratore di sistema

4. Analisi dei rischi che incombono sui dati

- 4.1 Descrizione stato attuale
 - 4.1.1 Descrizione dell'edificio e dei locali dove avviene il trattamento
 - 4.1.2 Gestione delle chiavi
 - 4.1.3 Rilevazione struttura sistema informatico
 - 4.1.4 Videosorveglianza
- 4.2 Analisi dei rischi
 - 4.2.1 Rischi riguardanti le basi di dati trattate senza strumenti informatici
 - 4.2.2 Rischi per il sistema informativo automatizzato

5. Misure da adottare per garantire l'integrità e la disponibilità dei dati

- 5.1 Misure fisiche
 - 5.1.1 Sicurezza di area
 - 5.1.2 Sicurezza degli archivi
 - 5.1.3 Attuazione degli adeguamenti riferiti alle misure fisiche
- 5.2 Misure informatiche
 - 5.2.1 Sistema di autenticazione
 - 5.2.2 Sistema di autorizzazione
 - 5.2.3 Altre misure
 - 5.2.4 Attuazione degli adeguamenti riferiti alle misure informatiche
- 5.3 Misure organizzative

6. Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di affidamento del trattamento a soggetti esterni

- 6.1 Affidamento a persone fisiche
- 6.2 Affidamento a persone giuridiche

7. Modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

8. Interventi formativi

- 8.1 Interventi formativi iniziali
- 8.2 Interventi formativi al momento dell'ingresso in servizio
- 8.3 Interventi formativi di aggiornamento

9. Misure specifiche per i dati personali idonei a rivelare lo stato di salute

| | | |
|-------------------------------|--|-----------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 2 di 40 |

1 Introduzione

Il presente **Documento Programmatico sulla Sicurezza** definisce lo stato di attuazione nel comune di Monte Argentario per quanto disposto dal D. Lgs. 30 giugno 2003 n°196 Codice in materia di protezione dei dati personali agli articoli 31, 33, 34 e 35 e dal Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Codice), .

Il contenuto di quanto segue si riferisce alla struttura organizzativa e funzionale del Comune di Monte Argentario, come definita dalla delibera della G.C. n. 116 del 14.10.2008 "Proposta di deliberazione per l'introduzione di modifiche alla struttura organizzativa dell'amministrazione comunale".

Il Comune di Monte Argentario ha definito il "Regolamento comunale per l'uso degli strumenti informatici, della posta elettronica e internet da parte dei dipendenti", entrato in vigore nel corso dell'anno 2008.

Sulla materia il Comune di Monte Argentario aveva provveduto, per l'anno 2009, alla revisione e aggiornamento del Documento programmatico sulla sicurezza con delibera della Giunta Municipale n. 79 del 30.03.2009.

| | | |
|-------------------------------|--|------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 3 di 40 |

2 Elenco dei trattamenti di dati personali

Questo comune effettua il trattamento di dati esclusivamente per lo svolgimento delle funzioni istituzionali che gli sono proprie attraverso la realizzazione dei diversi procedimenti amministrativi. Nel trattamento dei dati il Comune di Monte Argentario osserva i presupposti ed i limiti definiti dal Codice, dalla legge e dai regolamenti.

2.1 Dati trattati dal personale interno

I trattamenti dei dati personali effettuati in questa Amministrazione sono da ricondursi a quelli necessari per la esecuzione dei procedimenti amministrativi affidati ai servizi così come definito in modo analitico nel Provvedimento del Sindaco del 10 maggio 2000 "Definizione per ogni singola struttura organizzativa delle relative responsabilità gestionali".

Il trattamento dei dati sensibili e giudiziari è disciplinato dall'apposito Regolamento, emanato con Deliberazione del Consiglio comunale nei tempi previsti dalla legge, come stabilito dagli articoli 20, comma 2, e 21, comma 2, del decreto legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali").

I trattamenti sono effettuati sia con l'ausilio di mezzi elettronici che senza l'ausilio di mezzi elettronici.

2.2 Dati il cui trattamento è affidato all'esterno

Le banche dati su supporto cartaceo e/o informatizzato, contenenti dati personali assegnati all'esterno per il trattamento sono:

| TIPI DI DATI O BANCHE DATI | SOGGETTO AFFIDATARIO | MODALITA' AFFIDAMENTO (contratto, convenzione) |
|--|---|---|
| Tutti i dati in nostro possesso dei cittadini | Publica Toscana S.r.l. | Contratto manutenzione software |
| Tutti i dati in nostro possesso dei cittadini | Datagroup S.r.l. | Contratto manutenzione software |
| Gestione contabilità | Publica Toscana S.r.l. Deltadator S.r.l. | Contratto manutenzione software |
| Tesoreria | Banca cassa di risparmio di Firenze | Convenzione |
| Contribuenti ICI | Halley | Contratto manutenzione software |
| Contribuenti tosap tarsu | Halley | Contratto manutenzione software |
| Contribuenti tarsu | Gerit M.P.S. | Convenzione |
| Dati personali e sensibili per gestione Cimiteri | Intesa SpA | Contratto |
| Dati personali per raccolta rifiuti | Co.Se.Ca. | Contratto |
| Tutti i dati normali e/o sensibili (se necessari per lo svolgimento dell'attività di refezione) | Coop Arcobaleno | Contratto |
| Dati personali ed indirizzi per notifica contravvenzioni | Maggioli | Convenzioni |

| | | |
|-------------------------------|--|------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 4 di 40 |

| Dati ordinari | Ditta Falaschi Luca | Convenzioni |
|--|--|--------------------|
| Dati connessi allo svolgimento di rapporti commerciali. Archivio elettronico e cartaceo | Soc. Coop. a r.l. USCITA di SICUREZZA | Convenzioni |
| Dati connessi allo svolgimento di rapporti commerciali. Archivio elettronico e cartaceo | Soc. DUSSMANN Srvce srl | Convenzioni |
| Dati connessi allo svolgimento di rapporti commerciali. Archivio elettronico e cartaceo | Confraternita Misericordia e SS. Sacramento | Convenzioni |
| Dati connessi allo svolgimento di rapporti commerciali. Archivio elettronico e cartaceo | Associazione Girotondo | Convenzioni |

Le convenzioni citate in precedenza regolano, per gli aspetti di cui al D.Lgs. 196/2003 le modalità di trattamento e di comunicazione dei dati personali comuni e sensibili.

| | | |
|-------------------------------|--|-----------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 5 di 40 |

3 Distribuzione dei compiti e delle responsabilità

Il Codice individua, oltre all'interessato (lettera i, comma 1 art. 4 del Codice), i soggetti che sono coinvolti nel trattamento dei dati personali:

- il **titolare**, cioè la persona fisica o giuridica che ha la responsabilità finale ed assume le decisioni fondamentali riferite al trattamento dei dati personali (articolo 28 del Codice);
- il **responsabile**, è la persona, dotata di particolari caratteristiche di natura morale e di competenza tecnica, preposta dal titolare al trattamento dei dati personali "ivi compreso il profilo della sicurezza"; possono essere nominati anche più responsabili in base ad esigenze organizzative (articolo 29 del Codice);
- l'**incaricato** è la persona fisica che materialmente provvede al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile se nominato (articolo 29 del Codice);

Il Provvedimento a carattere generale - 27 novembre 2008 del Garante per la protezione dei dati personali individua un nuovo soggetto

- l'**amministratore di sistema**, "figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti" , "amministratore di basi di dati, amministratore di rete e di apparati di sicurezza, amministratori di sistemi software complessi".

3.1 Individuazione ed attribuzioni del responsabile

Il comma 2 dell'articolo 30 del Codice così recita "*Se designato, il responsabile, deve essere nominato fra i soggetti che per esperienza capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza*".

Il Sindaco, nella sua qualità di titolare, ha deciso di individuare quali "responsabili del trattamento dei dati" i responsabili dei settori nei quali è articolata l'amministrazione comunale (come risulta dalla citata delibera della G.C. n. 116 del 14.10.2008 "Proposta di deliberazione per l'introduzione di modifiche alla struttura organizzativa dell'amministrazione comunale"), individuando fra i citati responsabili il Responsabile I settore – Segretario generale come **responsabile con funzioni di coordinamento**.

- I. Settore Ufficio di staff, stampa e comunicazione istituzionale** (Ufficio di staff del sindaco, URP, Ufficio stampa e comunicazione istituzionale, protocollo ed archivio, ufficio notificazioni, personale e risorse umane, contenzioso e contratti, servizi demografici e statistici, sistema informatico, caccia e pesca)
- II. Settore Servizi finanziari e patrimoniali** (Bilancio contabilità e programmazione finanziaria, provveditorato ed economato, demanio e demanio marittimo, tributi, servizi di controllo e di revisione contabile, patrimonio - gestione catenarie)
- III. Settore Urbanistica, edilizia, politiche per il territorio e lo sviluppo, lavori pubblici servizi tecnici, infrastrutture** (Pianificazione territoriale ed urbanistica – Ufficio aree protette, edilizia privata – sportello unico per l'edilizia, attività produttive e commercio SUAP, Opere e lavori pubblici, ufficio espropri, servizi manutentivi ed ambientali, parchi e verde pubblico, servizi cimiteriali, protezione civile, servizio di prevenzione e protezione)
- IV. Settore Servizi sociali – culturali ed educativi** (pubblica istruzione, sport e turismo, servizi sociali e sanità, cultura e spettacolo, edilizia economica e popolare – politiche per la casa)

| | | |
|-------------------------------|--|------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 6 di 40 |

V. Settore Corpo di polizia municipale (Polizia locale, fiere e mercati)

Il **responsabile con funzione di coordinamento**, è preposto dal titolare, alla funzione di coordinamento tecnico di tutti i responsabili, interni ed esterni, e collabora con il titolare stesso per la realizzazione degli adempimenti generali disposti dal decreto legislativo 30 giugno 2003, n° 196, quali:

- a) predisposizione delle nomine a responsabile e verifica annuale delle stesse;
- b) definizione ed aggiornamento del Documento programmatico per la sicurezza;
- c) verifiche periodiche sulla attivazione e sulla efficacia delle misure di sicurezza;
- d) verifiche periodiche sull'operato dei responsabili;
- e) tenuta del fascicolo riguardante gli atti previsti dal Codice;
- f) nomina dell'incaricato con funzioni di amministratore di sistema
- g) controllo e verifica dell'attività dell'incaricato con funzioni di amministratore di sistema.

Gli schemi degli atti di nomina del responsabile del trattamento dei dati del responsabile del trattamento dei dati con funzioni di coordinamento e dell'incaricato con funzioni di amministratore di sistema sono allegati alla *Delibera della giunta Municipale* n. 283 del 28.12.2005.

3.2 I responsabili esterni

Il comune di Monte Argentario si avvale per l'espletamento di alcune attività di soggetti esterni; quando i dipendenti di tali soggetti, nell'ambito del servizio prestato, hanno accesso ad aree contenenti archivi di dati personali e/o a dati personali, i legali rappresentanti dei citati soggetti saranno nominati dal titolare **responsabili esterni del trattamento dati**.

Lo schema dell'atto di nomina del responsabile esterno del trattamento dei dati è inserito nella Delibera della Giunta Municipale n. 283 del 28.12.2005.

3.3 Gli incaricati

Sono individuati quali "incaricati del trattamento dati" i dipendenti del Comune, addetti ai Servizi che costituiscono i vari Settori, che abbiano accesso, per la loro funzione, a dati personali.

Sono da considerarsi incaricati a tutti gli effetti anche i dipendenti temporanei, il personale a convenzione ed altri soggetti che hanno accesso per il loro incarico a dati personali.

Gli incaricati sono nominati dai responsabili del trattamento dati dei settori di competenza.

I dipendenti da soggetti esterni che operano nel Comune, per l'espletamento di servizi manutentivi o altro, saranno identificati ed incaricati con specifico atto dal datore di lavoro, previamente nominato dal titolare responsabile esterno.

Lo schema dell'atto di nomina dell'incaricato del trattamento dei dati è inserito nell'allegato A al presente Documento.

3.4 L'amministratore di sistema

Il Garante con il Provvedimento a carattere generale - 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (G.U. n. 300 del 24 dicembre 2008) richiama l'attenzione di enti, amministrazioni, società private sulla figura professionale dell'amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

In sostanza il provvedimento dispone quanto segue.

a. Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve

| | | |
|-------------------------------|--|------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 7 di 40 |

fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

b. Designazioni individuali

La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

c. Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti.

d. Servizi in outsourcing

Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

e. Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

f. Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Ordinariamente la gestione del sistema informatico dell'ente è affidata ad un incaricato con funzioni di amministratore di sistema dipendente dell'ente.

Lo schema dell'atto di nomina dell'incaricato con funzione di amministratore di sistema è inserito nell'allegato A al presente Documento.

Nel fascicolo privacy viene conservata specifica documentazione che attesti capacità, esperienza e affidabilità dell'amministratore di sistema.

Per la manutenzione delle procedure gestionali informatiche l'amministrazione si avvale delle società specializzate fornitrici, nominate responsabili esterni, con le quali ha stipulato specifiche convenzioni.

Il responsabile con funzioni di coordinamento verificherà annualmente, alla data del rinnovo del DPS, l'operato degli amministratori di sistema attraverso le seguenti modalità:

- acquisizione di una relazione dell'amministratore di sistema dove vengano puntualmente descritte le attività realizzate sul sistema informatico;
- analisi dei rapporti operativi cartacei, per gli interventi in situazione, e elettronici (e.mail) per i servizi in Outsourcing;

| | | |
|-------------------------------|--|------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 8 di 40 |

- analisi del registro degli interventi, dei guasti e malfunzionamenti;

Per quanto riguarda la registrazione degli accessi (file di log), premesso che è prevista dal presente documento e attiva una procedura di autenticazione per gli accessi al sistema informatico dell'Amministrazione, è in fase di valutazione da parte del titolare l'acquisizione di un sistema che risponda alle prescrizioni definite dal Garante al punto f del citato provvedimento. Nelle more dell'attivazione di tale sistema il Responsabile con funzioni di coordinamento ha provveduto a definire una procedura adeguata al raggiungimento dello scopo individuato dal provvedimento del Garante. La procedura consiste in:

- autenticazione che viene registrata automaticamente dal sistema con indicazione dell'ora di inizio e fine dell'accesso;
- registrazione su un registro cartaceo degli accessi con la descrizione dell'evento che li ha generati, le operazioni effettuate, i dati identificativi dell'amministratore di sistema.

| | | |
|-------------------------------|--|------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 9 di 40 |

4 Analisi dei rischi che incombono sui dati

Per procedere all'analisi dei rischi che incombono sui dati è necessario descrivere ed analizzare la situazione attuale della amministrazione comunale.

4.1 Descrizione dello stato attuale

I dati che seguono sono relativi a una rilevazione effettuata nel marzo 2010.

4.1.1 Descrizione dell'edificio e dei locali dove avviene il trattamento

I locali ove avviene il trattamento dei dati sono:

- A. la sede Municipale posta in Porto S. Stefano**
- B. la sede della Polizia Municipale posta in Porto S. Stefano**
- C. la sede della Delegazione comunale posta in Porto Ercole**
- D. archivio storico e di deposito posto in Porto S. Stefano (loc. Appetito alto)**
- E. archivio di deposito posto in Porto S. Stefano (loc. Campone)**
- F. anagrafe e tributi in Porto S. Stefano**

Descrizione generale dell'edificio

A) Sede Municipale

E' costituita da un unico fabbricato, di quattro piani fuori terra, così distribuiti:
Accesso unico dalla piazza antistante il palazzo costituito da un portone in legno massiccio dotato di serratura ordinaria.

Piano terra

tramite il portone principale, si accede all'atrio ove è presente uno sportello a vetri, che dà su un piccolo vano con accesso esclusivo che ospita personale di vigilanza durante l'orario di apertura al pubblico; il corridoio che da accesso alla scala principale, all'ascensore e agli uffici è separato dall'atrio da una porta a vetri con serrature efficienti: aperta durante l'orario di apertura degli uffici al pubblico, viene chiusa in orario di chiusura degli uffici e aperta solamente a richiesta; il piano ospita i seguenti uffici: Servizi Sociali, Pubblica istruzione - Cultura, Commercio, SUAP, Ormezzi, Casa, l'Archivio urbanistica, Protocollo ed il locale adibito a sala macchine del sistema informatico; i locali sono dotati di porte in resina di buona consistenza e serrature ordinarie tipo Yale, le finestre accessibili per posizione sono munite di grate metalliche.

Piano primo

vi si accede esclusivamente mediante la scala centrale e l'ascensore dai quali, attraverso una porta in vetro con serratura ordinaria, si accede al corridoio nel quale si affacciano la Sala consiliare e gli Uffici dei messi comunali, Economato, Patrimonio e Finanziari tutti dotati di porte di buona consistenza con serrature ordinarie e finestre inaccessibili per posizione.

Piano secondo

vi si accede esclusivamente mediante la scala centrale e l'ascensore dai quali, attraverso una porta in vetro con serrature ordinarie, si accede al corridoio nel quale si affacciano l'Ufficio del Sindaco e la sua segreteria, muniti di porte con serrature normali e finestre inaccessibili; al piano si trovano l'Ufficio del Segretario Comunale e gli Uffici Segreteria, Affari Generali, Personale, Demanio, l'Ufficio Contratti, tutti dotati di porte con serrature normali e finestre inaccessibili.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 10 di 40 |

Piano terzo

vi si accede esclusivamente mediante la scala centrale e l'ascensore dai quali, attraverso una porta in vetro con serrature ordinarie, si entra nel corridoio intermedio che da accesso agli uffici del Settore Urbanistica, edilizia, politiche per il territorio e lo sviluppo, lavori pubblici servizi tecnici, infrastrutture, tutti dotati di porte di buona consistenza con serrature ordinarie e finestre inaccessibili per posizione.

N.B.

* Nei corridoi ai vari livelli sono presenti armadi contenenti documentazione amministrativa ed anche dati personali.

* La sala consiliare, collocata al primo piano, viene utilizzata anche fuori dell'orario di apertura dal pubblico per attività diverse (conferenze, riunioni, etc) organizzate anche da soggetti privati.

B) Sede della Polizia Municipale

è collocata in un fabbricato, composto da due piani, occupati totalmente dal servizio in questione, e così suddivisi.

Piano terra

con accesso dalla pubblica via mediante portone in alluminio e vetro con serrature e consistenza mediocri, si accede all'ingresso principale sul quale si affacciano: sul fronte la scala in metallo che porta al piano superiore; sul lato destro un locale archivio munito di porta e finestre (sulla sede stradale) in alluminio e vetro di mediocre consistenza e tenuta; sul lato sinistro altro locale adibito ad ufficio (presidiato durante l'orario di lavoro da personale) dal quale, mediante porta secondaria di mediocre tenuta, si accede all'ampio locale adibito a magazzino e garage che dispone di quattro aperture sulla sede stradale dotate di porte in metallo basculanti con serrature e tenuta non adeguate;

Piano primo

vi si accede esclusivamente dalla scala suddetta, ed ospita sei locali adibiti ad uffici i quali dispongono di porte interne, in alluminio e vetro, ordinarie e di finestre esterne, tutte sulla pubblica via, con tenuta non adeguata.

Nell'edificio è presente un sistema generale di allarme.

C) Sede della Delegazione Comunale di Porto Ercole

fa parte di un fabbricato a più piani, con due accessi esterni, uno dalla via superiore e l'altro dalla piazza sottostante ed ospita:

al piano terra: due locali ufficio ed un magazzino, in uso alla Polizia Municipale e di finestre, accessibili, (affacciate direttamente sulla pubblica via); la porta che da accesso al locale utilizzato dalla Polizia Municipale presenta adeguati caratteri di sicurezza; l'altra porta in legno e vetro si presenta con serrature e tenuta non adeguate.

al piano primo: locali in uso all'Azienda USL e un ufficio turistico nel quale non sono trattati dati personali;

al piano secondo: alcuni locali destinati ad uffici comunali (servizi anagrafici e tributi), ai quali si accede direttamente dalla scala; la porta di accesso agli uffici anagrafici presenta adeguati caratteri di sicurezza; la porta dell'ufficio tributi non è sicura; le finestre degli uffici appaiono difficilmente accessibili dall'esterno per posizione;

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 11 di 40 |

negli uffici sono presenti arredi, che contengono anche dati personali, con diverse caratteristiche di sicurezza e attrezzature informatiche in rete (mediante linea protetta) con il sistema informatico comunale;

durante l'orario di apertura al pubblico l'ingresso ai locali è costantemente presidiato dal personale di servizio.

al piano terzo: locali a servizio della biblioteca.

Appare evidente, considerato l'uso plurimo dei locali, la precaria condizione della sicurezza dei locali stessi.

D) Archivio storico e di deposito in Porto S. Stefano (loc. Appetito alto)

I locali che ospitano l'archivio storico e una piccola parte del deposito sono dotati di impianto antincendio e porta rei tagliafuoco. Non è presente un sistema di allarme.

E) Archivio di deposito in Porto S. Stefano (loc. Campone)

I locali che ospitano buona parte dell'archivio di deposito sono in fase di allestimento per adeguarli agli standard di sicurezza necessari.

F) Anagrafe e tributi in Porto S. Stefano

I locali che ospitano l'Uff. anagrafe, stato civile e leva e l'Uff. tributi sono comunicanti (mediante una scalinata interna) e collocati in un edificio a cui si accede da Corso Umberto I, attraverso una porta in alluminio e vetri antisfondamento, e da via XX Settembre mediante un portone in legno con serratura antiscasso. L'Uff. anagrafe collocato al pian terreno consta di tre locali (stato civile, elettorale e leva, saletta server) ed è costantemente presidiato dal personale durante l'orario di apertura al pubblico. L'Uff. tributi collocato al primo piano si compone di quattro locali più locale per servizi igienici, dotato di una finestra accessibile per posizione; durante l'orario di apertura al pubblico l'ingresso ai locali è costantemente presidiato dal personale di servizio. Nell'Uff. anagrafe è presente un sistema di allarme.

Nei locali descritti in precedenza sono presenti arredi di diverse tipologie: scrivanie, schedari metallici, armadi in legno, in metallo e in metallo e vetro, solo in parte provvisti delle necessarie caratteristiche di sicurezza in relazione ai documenti contenuti; le serrature, ove presenti, sono spesso inefficienti e/o utilizzate in modo non corretto.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 12 di 40 |

4.1.2 Gestione delle chiavi

Chiavi di accesso agli edifici

Data la distribuzione degli uffici dell'Amministrazione in più edifici; e la utilizzazione di alcune aree e locali da parte di soggetti esterni, la gestione delle chiavi di accesso ai diversi edifici e alle aree interessate appare oggettivamente complessa.

Attualmente nell'Ente non è definita formalmente una modalità unica per la gestione delle chiavi; per cui la situazione, in ordine alla sicurezza, appare differenziata a seconda degli edifici e degli uffici; in alcuni casi sono state adottate, da parte dei dirigenti, procedure di gestione (verbali di affidamento, procedure per la custodia delle copie di sicurezza), più spesso le chiavi sono affidate senza formalità al personale di ufficio, agli amministratori, a soggetti esterni autorizzati.

Le chiavi di accesso al palazzo municipale vengono affidate, in genere senza formalità, a soggetti esterni quando nella sala consiliare si tengono iniziative "esterne" (mostre, convegni, conferenze).

Chiavi di accesso agli uffici

Le chiavi degli uffici dove vengono trattati dati sono gestite dai dirigenti e dai responsabili dei diversi servizi ed affidate, salvo eccezioni, senza formalità agli incaricati.

Chiavi degli archivi

Le chiavi degli archivi che contengono dati personali sono gestite dai responsabili e da questi affidate agli incaricati in generale senza formalità; non sempre sono disponibili copie di sicurezza.

Le porte della quasi totalità degli uffici vengono chiuse dagli incaricati alla fine dell'orario di lavoro.

Alla società incaricata delle pulizie sono state affidate senza formalità le chiavi degli edifici e degli uffici.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 13 di 40 |

4.1.3 Rilevazione struttura sistema informatico

RILEVAZIONE STRUTTURA SISTEMA INFORMATIVO

1-Tipologia della rete

- Tre reti a stella collegate in fibra ottica
- Rete a stella della sede decentrata di Porto Ercole collegata con HDSL in WPN
- Rete Wireless per collegare il portatile (utilizzato esclusivamente dall' Amministratore di sistema)

2- Tipologia delle risorse hardware

N° 7 Server Windows XP 2003
 N° 90 Clients
 N° 5 Portatili
 N° 5 macchinette per il controllo orari

3- Collocazione server

I server sono collocati in locali ad uso esclusivo

4- Accesso alle risorse Internet

Tramite Gateway (sia nella sede principale che in quella distaccata di Porto Ercole)

5- Posta elettronica

Provider Aruba

TIPOLOGIA DELLE RISORSE SOFTWARE

6- Sistema operativo usato sul server

Windows XP 2003
 Linux SuSE 10

7-Sistemi operativi usati sui client licenze di Office Automation Microsoft Licenze antivirus Elenco procedure

Windows XP SP2/SP3

 Microsoft Office
 Open Office

 Kaspersky

 CIVILIA OPEN

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 14 di 40 |

| |
|---|
| <p>HALLEY (Servizio ICI, TARSU)</p> <p>DELTADATOR (Segreteria, Anagrafe, Ragioneria, Ufficio tecnico)</p> <p>MAGGIOLI (Vigili urbani)</p> |
|---|

8- Supervisore di rete

| |
|----|
| Si |
|----|

9- Progetto e certificazione della rete

| |
|----|
| Si |
|----|

10- Planimetria della rete

| |
|----|
| Si |
|----|

11- Uso della rete

| |
|--|
| <p>Normali procedure di lavoro</p> <p>Archiviazione dati</p> |
|--|

12- Interventi di formazione del personale

| |
|-----------------------------------|
| Solo per alcune figure specifiche |
|-----------------------------------|

13- Assegnazione di nomi logici per le periferiche di rete

| |
|----|
| SI |
|----|

14- Assegnazione delle password di accesso alle singole macchine

| |
|----|
| SI |
|----|

15- Assegnazione dei codici identificativi personali

| |
|----|
| SI |
|----|

16- Collaboratori esterni o temporanei che hanno accesso alla rete

| |
|---|
| <p>PUBLICA (Sesto Fiorentino)</p> <p>MAGGIOLI</p> <p>HALLEY</p> |
|---|

PREVENZIONE DELLA PERDITA DEI DATI

17- Software antivirus

| |
|---|
| <p>Sul server e sui clients</p> <p>Modalità aggiornamento: automatico</p> |
|---|

18- Incarico formale dell'esecuzione dei backup

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 15 di 40 |

Procedure centralizzate e documenti residenti nei clients:

E' presente un incaricato

Documenti residenti nei portatili:

Il salvataggio viene effettuato in modo non formale

19- Supporto sul quale viene effettuato il backup

Procedure centralizzate

DVD

NAS 1 tera (salvataggio quotidiano, decentrato rispetto al server)

Documenti residenti nei clients

Nastro

20- Libro mastro della programmazione dei backup

File di log del sistema

21 – Contenitore e locale dove vengono custodite le copie di backup

Luogo e contenitore sicuri

22- Strumenti di difesa antintrusione

ROUTER ADSL

FIREWALL Kerio

23- Gruppo/gruppi di continuità

In via di installazione

24- Manutenzione delle risorse hardware e software

Fornitori a chiamata

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 16 di 40 |

4.1.4 Videosorveglianza

Nel comune di Monte Argentario sono in via di attivazione alcuni impianti di videosorveglianza:

- N° 4 impianti di videosorveglianza per il controllo dell'ingresso alle ZTL costituiti da telecamere fisse (senza possibilità di brandeggio e zoom) collocate in:

Porto S. Stefano

Varco Pilarella

- Piazza Vittorio Emanuele
- Piazza dei Rioni

Varco corso Umberto

- Incrocio via del Cetino
- Incrocio via S.Stefano

Porto Ercole

- Via delle buche incrocio Via Caravaggio
- Lungomare strozzi incrocio via della marina
- Arco di via Italia

Le immagini verranno registrate in un apparato collocato nella sede della Polizia Municipale. Il sistema rileverà in modo automatico le targhe degli autoveicoli in transito solo in caso di infrazione; le registrazioni saranno conservate solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso, l'accesso ai dati è consentito esclusivamente a fini di polizia giudiziaria o di indagine penale.

- Impianto di videosorveglianza finalizzato alla prevenzione di atti vandalici e per rilevare gli autori di danneggiamenti a strutture o cose costituito da n° 4 telecamere con possibilità di brandeggio a 360° e zoom collocate in:

Porto S. Stefano

- Piazza Vittorio Emanuele
- Torre faro piazzale Candi

Porto Ercole

- Via delle buche incrocio Via Caravaggio
- Torre faro molo distributore API

Le immagini verranno visualizzate su un monitor e registrate in un apparato collocato nella sede della Polizia Municipale. La registrazione viene conservata per 7 giorni e quindi cancellata in modo automatico.

Con appositi atti l'Amministrazione definirà, in conformità con quanto disposto dal Provvedimento generale del Garante per la protezione dei dati personali 29 aprile 2004, la "documentazione delle scete" ed un regolamento per la gestione degli impianti.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 17 di 40 |

4.2 Analisi dei rischi

4.2.1 Rischi riguardanti le basi di dati trattate senza strumenti informatici

I rischi sotto elencati riguardano le attività di trattamento dei dati effettuate con mezzi manuali:

- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, ecc.:**
 - per la Sede Municipale, la Delegazione Comunale di Porto Ercole e gli archivi, data la collocazione dei locali, i rischi di allagamento per cause naturali o di guasti alle condotte idriche e termiche appaiono pressoché nulli; per la sede della Polizia Municipale i rischi di allagamento per cause naturali appaiono presenti per gli ambienti collocati al piano strada e di scarsa rilevanza per gli uffici collocati al primo piano.
 - per quanto riguarda i rischi di furto e/o danneggiamento per atti vandalici occorre distinguere tra le varie sedi: per la sede municipale il presidio dell'accesso all'edificio da parte del personale, durante l'orario di apertura degli uffici, e la presenza di misure antintrusione, (grate metalliche alle finestre del piano terra) abbattano notevolmente il rischio che però permane, dopo la chiusura degli uffici, sia a causa della mancanza di un sistema generale di allarme e della modesta affidabilità della porta principale di accesso che per l'utilizzo di alcuni locali da parte di soggetti privati; per la sede dell'anagrafe e tributi il rischio è di livello basso visto che è presente un sistema di allarme; per la sede della Polizia Municipale i rischi sono bassi per la presenza di un sistema di allarme; per alcuni locali dove è collocata la sede della Delegazione Comunale di Porto Ercole e degli archivi i rischi sono elevati per l'assenza di dotazioni antintrusione (finestre facilmente accessibili, porta non sicura);
- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
 - tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.
 - per l'archivio storico esistono rischi rilevanti a causa della situazione dei locali.
- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
 - per la sede municipale la situazione appare critica ed il rischio molto elevato visto che nei corridoi sono collocati contenitori, spesso non adeguati dal punto di vista della sicurezza, che ospitano banche dati anche di natura personale;
- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
 - il rischio è di natura media in quanto la maggioranza del personale non è stata sensibilizzata e formata, in modo specifico, sui temi di cui si tratta;
- **connessi all'utilizzo di archivi e contenitori con serrature:**
 - gli archivi ed i contenitori delle banche di dati personali vengono progressivamente adeguati alle disposizioni di legge, sono state adottate misure tecniche ed organizzative tali da abbattere notevolmente il rischio che, attualmente, appare nel complesso medio.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 18 di 40 |

- **connessi con la gestione delle chiavi di accesso:**

- l'attuale gestione presenta alcuni problemi in ordine alla sicurezza in particolare riguardo alla procedura di affidamento (non formale) e alla gestione delle copie di sicurezza.

4.2.2 Rischi per il sistema informativo automatizzato

L'analisi dei rischi consiste nella individuazione degli elementi del sistema informativo automatizzato che necessitano di protezione e delle minacce cui gli stessi possono essere sottoposti, tenendo conto del fattore tecnologico e del fattore umano.

Le principali fonti di rischio per il sistema informatico sono aggregabili, ai fini della analisi oggetto del presente paragrafo, nel modo che segue:

FR1 - maltempo, inondazioni, fulmini, terremoti, fuoco, attentati

FR2 - guasti hardware, caduta di corrente, omissioni hardware, errori e difetti software, sabotaggi, haking, programmi software maligni (malware,virus, worm)

FR3 - comportamenti errati, cattiva organizzazione, errata logistica

Il sistema informatico dell'Amministrazione, come descritto al precedente punto 4.1.3, è distribuito nei locali dove si esegue il trattamento dati senza l'ausilio di strumenti cartacei per cui per quanto riguarda i rischi compresi nel gruppo FR1 si fa riferimento a quanto detto al precedente punto 4.2.1.

Riguardo alle fonti di rischio comprese nel gruppo FR2, fino ad oggi anche da una analisi della serie storiche riguardanti il sistema informatico emerge quanto segue:

- o non si sono registrati consistenti guasti hardware, anche per la continua manutenzione dello stesso e l'uso di macchine affidabili;
- o nella zona in cui insistono i locali che ospitano il sistema informatico non si verificano frequentemente cadute di corrente, tuttavia il rischio è presente dato che il sistema è sprovvisto di gruppi di continuità (acquistati ma non ancora installati per problemi tecnici);
- o il sistema consente il salvataggio dei dati attraverso il server per gli archivi delle procedure gestionali e per gli archivi residenti nei singoli clients;
- o il server e i clients sono dotati di antivirus che viene aggiornato via Internet quotidianamente in modo automatico;
- o Riguardo il rischio di accesso abusivo, con i rischi connessi quali conoscenza dati a persone non autorizzate, distruzione o perdita totale, danneggiamento dei dati ecc, fino ad oggi non si sono registrati eventi dannosi; in ogni modo il sistema non appare vulnerabile sia perchè si è provveduto all'assegnazione di codici identificativi personali e password di accesso, sia per la presenza di strumenti di difesa antintrusione (FIREWALL Hardware e Software).

Per le fonti di rischio comprese nel gruppo FR3 dall'analisi della rilevazione effettuata risulta quanto segue.

Le credenziali di autenticazione, consistenti in un codice per l'autenticazione associato ad una parola chiave sono gestite in modo corretto.

Circa il salvataggio dei dati, relativo alle banche dati delle procedure centralizzate e a quelle residenti nei singoli clients, il rischio di perdita di dati appare di livello basso visto che è stata attivata una procedura formale di backup.

Per quanto riguarda la procedura per la manutenzione dei programmi gestionali realizzata dai fornitori, in presenza o "da remoto", sussiste il rischio di accesso non autorizzato ai dati personali contenuti nei data base; il rischio appare di bassa entità considerato che l'accesso viene autorizzato di volta in volta dall'amministratore di sistema.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 19 di 40 |

5 Misure da adottare per garantire l'integrità e la disponibilità dei dati

5.1 Misure fisiche

I requisiti di sicurezza fisica sono tesi a:

- proteggere le persone che operano sui sistemi,
- proteggere le aree
- proteggere gli archivi.

5.1.1 Sicurezza di area

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza degli archivi e delle attrezzature informatiche rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

Adeguamento 1

Dotare le porta di accesso del Palazzo municipale e delle sedi distaccate di serrature efficienti e sicure (di tipo certificato) e fornire le finestre accessibili per posizione di misure antintrusione. Installare, nelle sedi dove il rischio di intrusione dall'esterno è elevato le opportune protezioni.

Adeguamento 2

Provvedere a una gestione "sicura" delle chiavi di accesso all'edificio comunale, come descritto al punto 4.1.2, attraverso l'individuazione

- dei soggetti preposti alla custodia delle copie di sicurezza
- di luoghi sicuri e contenitori idonei ove custodire le chiavi e le copie di sicurezza delle stesse
- dei soggetti affidatari
- di una corretta e efficace procedura di affidamento

Adeguamento 2/1

Dotare le porte di accesso agli uffici di serrature efficienti e sicure; provvedere alla gestione delle chiavi attraverso misure che identifichino e responsabilizzino i soggetti interni cui vengono affidate.

Adeguamento 2/2

Posizionare telefax, fotocopiatrici e stampanti di rete in modo tale da impedirne l'accesso e la visione al pubblico.

5.1.2 Sicurezza degli archivi

Adeguamento 3

Spostare in luogo "sicuro", o dotare di serrature efficienti, i contenitori di dati personali collocati in spazi accessibili al pubblico.

Adeguamento 4

Dotare ogni posto di lavoro ove opera un incaricato del trattamento dati sensibili e giudiziari di almeno un contenitore (cassetto, armadio) con serratura efficiente e sicura. Provvedere in modo corretto alla gestione delle chiavi (affidamento formale, custodia della copia da parte del responsabile del servizio).

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 20 di 40 |

Adeguamento 4/1

Le banche di dati personali (sensibili e non) devono essere contenute in contenitori adeguati (schedari, armadi) dotati di serratura efficiente e sicura. Provvedere in modo corretto alla gestione delle chiavi (affidamento formale, custodia della copia da parte del responsabile del servizio).

Adeguamento 4/2

- a) Devono essere indicati con adeguata segnaletica i locali interdetti al pubblico.
- b) Nei locali accessibili al pubblico deve essere delimitata l'area di accesso.
- c) Nei locali accessibili al pubblico per i quali non è possibile, per ragioni strutturali delimitare l'area di accesso, gli utenti sono ammessi uno alla volta adottando opportune misure organizzative (comunicazioni scritte, segnaletica o altro)

Adeguamento 4/3

Per i locali dell'archivio come prescrive anche il DPR 445/2000, il responsabile con funzioni di coordinamento autorizzerà per scritto l'accesso ed i trattamenti consentiti.

5.1.3 Attuazione degli adeguamenti riferiti alle misure fisiche

- L'attuazione degli adeguamenti 1, 2/1, 4 sarà effettuata a cura del Servizio Lavori Pubblici e Tecnico-manutentivo.
- L'attuazione degli adeguamenti 2 e 4/3 dovrà essere effettuata dal responsabile con funzioni di coordinamento, gli adeguamenti 2/2, 3, 4/1, 4/2 sarà curata dai responsabili competenti.

5.2 Misure informatiche

Il campo di applicazione della Sicurezza Logica riguarda la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Il Disciplinare tecnico in materia di misure minime di sicurezza, allegato B al Codice, prescrive l'adozione di alcune modalità tecniche che in questa Istituzione si sintetizzano come segue.

5.2.1 Sistema di autenticazione

Adeguamento 5

Devono essere rese operative per gli incaricati di trattamento le credenziali di autenticazione.

Le credenziali per l'autenticazione consistono nel sistema informatico attualmente in uso, in coerenza con quanto prescritto dal Disciplinare tecnico – allegato B al Codice punto 2, da un codice per l'identificazione dell'incaricato associato a una parola chiave.

La gestione del sistema di autenticazione informatica, per gli incaricati, sarà disposto dall'incaricato con funzioni di Amministratore di sistema come segue:

- a) La parola chiave viene assegnata dal responsabile all'incaricato all'avvio dell'applicazione delle norme definite dal presente Documento o all'atto del primo conferimento dell'incarico.
- b) La parola chiave è modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi.
- c) In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
- d) La parola non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- e) Ad ogni modifica della parola chiave, la parola chiave scelta dall'incaricato è inserita in una busta sigillata con all'esterno dati identificativi dell'interessato e la data di consegna; la busta sarà consegnata al responsabile con funzioni di coordinamento che la custodirà garantendo la segretezza del contenuto.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 21 di 40 |

- f) In caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema il responsabile con funzioni di coordinamento potrà accedere alla credenziale, provvedendo ad avvertire tempestivamente l'incaricato.

Adeguamento 5.1

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'uso della componente riservata della credenziale per l'autenticazione (punto 10 del Disciplinare Tecnico in materia di misure minime di sicurezza), il responsabile con funzioni di coordinamento definisce la procedura con la quale il titolare può assicurarsi la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento del responsabile con funzioni di coordinamento stesso.

5.2.2 Sistema di autorizzazione

Adeguamento 6

La gestione del sistema di autorizzazione, previsto per le procedure informatiche centralizzate viene disposto dal responsabile, per il servizio di competenza.

I profili di autorizzazione sono individuati e configurati all'avvio dell'applicazione delle norme definite dal presente Documento, su indicazione del responsabile di settore, dall'incaricato con funzioni di amministratore di sistema.

5.2.3 Altre misure

Adeguamento 7

I responsabili redigono entro il 31 marzo di ogni anno, per la propria area di competenza, la lista degli incaricati di trattamento specificando l'ambito di trattamento consentito ed i relativi profili di autorizzazione.

Almeno annualmente sarà verificata da parte dei responsabili, per la propria area di competenza, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Si allega al presente documento lo schema di scheda per l'individuazione degli incaricati di trattamento con strumenti informatici con i relativi profili di accesso.

La lista viene conservata dal responsabile con funzioni di coordinamento e copia della stessa inserita nel "fascicolo della privacy" a cura del responsabile con funzioni di coordinamento.

Adeguamento 8

Il responsabile con funzioni di coordinamento

- a) dispone che i dati personali siano protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
- b) impartisce istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale e provvede all'istituzione di un registro per il backup;
- c) provvede alla custodia in un luogo sicuro delle copie di backup;
- d) dispone la custodia dei supporti rimovibili contenenti dati personali individuando contenitori con idonee caratteristiche di sicurezza;
- e) dispone la distruzione di supporti rimovibili contenenti dati sensibili e giudiziari non più utilizzati;
- f) dispone e verifica la cancellazione di tutti i dati personali dagli strumenti informatici non più utilizzati o utilizzati in attività diverse da quelle amministrative.

Adeguamento 9

Il responsabile con funzioni di coordinamento quando l'Amministrazione si avvarrà di soggetti esterni per la fornitura di prodotti o servizi finalizzati alla realizzazione di misure minime di sicurezza, si farà consegnare dal soggetto medesimo una descrizione scritta dell'intervento che ne attesti la conformità a quanto disposto dal disciplinare tecnico allegato B del Codice.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 22 di 40 |

Adeguamento 10

Per gli elaboratori portatili e gli elaboratori non in rete, se utilizzati per il trattamento dei dati, è necessario, in aggiunta agli adeguamenti precedenti, che l'incaricato con funzioni di amministratore di sistema provveda a:

- creare un registro con la lista aggiornata degli affidatari e degli utenti;
- impartire istruzioni per la realizzazione del salvataggio;
- provvedere all'addestramento degli utenti autorizzati all'utilizzo sicuro degli apparati con riferimento specifico alle misure minime di sicurezza in materia di trattamento dei dati personali;
- curare l'installazione di dispositivi aggiuntivi di sicurezza, con procedure di utilizzo, per diminuire il rischio di furto;

Adeguamento 11

Ripristinare l'efficienza dell'apparato di continuità dell'erogazione della corrente elettrica, già presente. e tenuta del registro delle prove di efficienza dell'apparato di continuità.

Adeguamento 12

Per quanto riguarda la registrazione degli accessi (file di log) operati dagli amministratori di sistema, come dispone il Provvedimento del Garante - 27 novembre 2008 il responsabile con funzione di coordinamento provvederà a completare l'attivazione di idonei strumenti tecnici ed organizzativi.

Adeguamento 13

Il responsabile con funzione di coordinamento definirà e renderà attiva una procedura finalizzata alla registrazione dei guasti, malfunzionamenti del sistema informatico e degli interventi effettuati sullo stesso. La procedura consiste sinteticamente

- nella segnalazione formale di guasti e malfunzionamenti da parte degli incaricati attraverso uno specifico modulo;
- nella registrazione da parte dell'amministratore di sistema delle operazioni effettuate dagli amministratori di sistema (interni o esterni).

Adeguamento 14

Provvedere a dotare di apposita segnaletica (conforme con quella indicata dal Garante) le aree sottoposte a videosorveglianza.

5.2.4 Attuazione degli adeguamenti riferiti alle misure informatiche

L'Amministrazione ha provveduto a realizzare gli adeguamenti da 5 a 10 al relativi sistema informatico; riguardo al punto 12 l'attivazione di uno strumento per la registrazione degli accessi conforme alla normativa, considerati gli aspetti tecnici ed economici, appare realizzabile in tempi brevi.

5.3 Misure organizzative

Accanto all'adozione di misure tecnologiche già illustrate, è necessario, come richiamato, vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo di sicurezza.

Gli aspetti organizzativi riguardano principalmente:

- la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo Sicurezza;
- l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 23 di 40 |

Un ulteriore aspetto inerente la Sicurezza Organizzativa è quello concernente i controlli sulla consistenza e sulla affidabilità degli apparati.

In ordine alla norme di comportamento, si rimanda a quanto è definito nei documenti di nomina per l'assegnazione di responsabilità ed incarichi ed a quanto specificato nell'allegato A.

I responsabili relativamente ai propri ambiti di competenza, aggiornano almeno annualmente la lista degli incaricati (redatta anche per classi omogenee di incarico) con i relativi profili di autorizzazione utilizzando gli allegati B e C.

In ordine a quanto disposto dal Garante con il Provvedimento a carattere generale - 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (G.U. n. 300 del 24 dicembre 2008), il titolare provvederà alla individuazione di responsabili e incaricati come specificato al punto 3.4 del presente documento e esplicitato nei relativi modelli di nomina di cui all'allegato A.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 24 di 40 |

6 Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di affidamento del trattamento a soggetti esterni

Nel caso di affidamento da parte dell'Amministrazione a soggetti esterni di attività che comportino trattamento dei dati conviene distinguere fra:

- a) affidamento a persone fisiche;
- b) affidamento a persone giuridiche.

6.1 Affidamento a persone fisiche.

Nel caso che il soggetto sia una persona fisica lo stesso sarà nominato, dal titolare o dal responsabile competente, incaricato di trattamento dati attraverso un atto di nomina che specifichi puntualmente le norme di comportamento da seguire.

Sarà cura del titolare e dei responsabili, per i settori di competenza, individuare i soggetti esterni che per l'espletamento di incarichi conferiti dall'Amministrazione devono avere accesso a dati personali.

Ove necessario il titolare o il responsabile competente provvederanno a informare l'incaricato sui contenuti fondamentali delle norme che disciplinano il trattamento dei dati personali.

Il titolare o il responsabile verificheranno periodicamente, nelle forme ritenute più opportune, sulla correttezza del trattamento, con particolare riferimento all'adozione delle misure minime di sicurezza, da parte degli incaricati.

6.2 Affidamento a persone giuridiche.

Nel caso che il soggetto cui viene affidato un incarico sia una persona giuridica la stessa sarà nominata dal titolare **responsabile esterno di trattamento dati**, attraverso un atto di nomina che specifichi puntualmente le norme di comportamento da seguire con specifico riferimento alle misure minime di sicurezza da adottare.

Il titolare vigilerà sulle attività relative al trattamento dipendenti dal responsabile esterno e si farà rilasciare dallo stesso una dichiarazione di conformità a quanto stabilito dalle norme di legge e dal presente documento.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 25 di 40 |

7 Modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Il responsabile con funzioni di coordinamento nel caso del verificarsi di eventi che provochino la distruzione od il danneggiamento dei dati personali contenuti nelle banche dati del sistema informatico, provvederà senza ritardo a ripristinare la funzionalità delle banche dati.

Il ripristino della disponibilità dei dati andati perduti a causa di eventi di diversa natura consiste di norma

- nella installazione del software di base, dei programmi, di tutti i file di dati,
- nella sostituzione di componenti hardware che hanno provocato la interruzione dei trattamenti.

La re-installazione del software di base, dei programmi di office automation e dei file di dati residenti nei PC sarà effettuata dall'incaricato con funzioni di amministratore di sistema.

La re-installazione del software di rete, dei programmi gestionali e dei file di dati residenti nel server sarà effettuato dal soggetto titolare della manutenzione software.

La sostituzione di componenti hardware non funzionanti sarà effettuato dal soggetto titolare della manutenzione hardware.

Nei contratti di manutenzione stipulati con i fornitori di software e hardware dovrà essere inserita una specifica clausola che consenta il ripristino della funzionalità del sistema informatico e della disponibilità dei dati entro il tempo stabilito dalla legge.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 26 di 40 |

8 Interventi formativi

8.1 Interventi formativi iniziali

In coerenza con quanto previsto dalle norme è necessario, insieme alla realizzazione degli adempimenti riguardanti la sicurezza del trattamento dei dati personali, provvedere alla formazione iniziale di tutto il personale in servizio.

Le norme, punto 19.4 del Disciplinare tecnico-Allegato B al Codice, prevedono che la formazione deve essere prevista all'ingresso in servizio e ogni volta che l'incaricato si trovi a trattare nuove tipologie di dati o utilizzi diverse modalità di trattamento.

I contenuti della formazione vengono individuati come segue:

- illustrazione e analisi del Codice e del contesto normativo di riferimento;
- analisi dettagliata del disciplinare tecnico – Allegato B al Codice;
- illustrazione della politica di sicurezza dei dati adottata nel Comune e sintetizzata nel presente documento;
- profili di responsabilità civile e penale.

I contenuti saranno affrontati in modo specifico per i responsabili interni e per la generalità degli incaricati.

8.2 Interventi formativi al momento dell'ingresso in servizio

Il personale che prende per la prima volta servizio nel Comune verrà (in)formato sui contenuti del Codice, anche attraverso la fornitura di materiale di sintesi, dal responsabile competente.

In sede di verifica dell'efficacia delle misure di sicurezza il responsabile con funzioni di coordinamento in accordo con l'incaricato con funzioni di Amministratore di sistema, qualora necessario, programmerà attività formative per il personale che ha preso servizio nella istituzione e che non è stato in precedenza sottoposto a formazione sui temi di cui si tratta.

Il personale a convenzione al momento dell'ingresso in servizio verrà (in)formato sui contenuti del Codice e sui doveri da esso derivanti, anche attraverso la fornitura di materiale informativo, di sintesi dal responsabile competente.

8.3 Interventi formativi di aggiornamento

In sede di verifica dell'efficacia delle misure di sicurezza, anche in relazione a novità che di dovessero presentare nelle norme di legge e/o in relazione all'evoluzione tecnica del settore, il titolare ed il responsabile programmeranno le necessarie attività formative.

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 27 di 40 |

9 Misure specifiche per i dati personali idonei a rivelare lo stato di salute

Questa istituzione tratta dati idonei a rivelare lo stato di salute esclusivamente per finalità previste dalla legge.

Secondo quanto prescritto dall'articolo 22 comma 7 del D. lgs 196/2003 i dati idonei a rivelare lo stato di salute *"sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo"*; inoltre il comma 7 dello stesso articolo dispone che i dati idonei a rivelare lo stato di salute, qualora contenuti in banche dati informatiche vengano trattati *"con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altre soluzioni, che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità"*.

Il trattamento dei dati di cui si tratta al momento è realizzato senza l'ausilio di strumenti elettronici,

a) Dati riguardanti il personale

I dati consistono essenzialmente in certificati medici, necessari per lo svolgimento di specifici procedimenti, consegnati o fatti pervenire all'ufficio personale

Dopo la ricezione, durante il trattamento (protocollazione etc) saranno inseriti in un contenitore chiuso riferito all'interessato e successivamente inseriti nel fascicolo personale, dove saranno conservati all'interno di una busta chiusa recante l'indicazione del contenuto separatamente dagli altri documenti.

b) Dati riguardanti interessati non dipendenti

I dati consistono essenzialmente in certificati medici, necessari per lo svolgimento di specifici procedimenti riferiti ai servizi sociali e ai servizi scolastici.

Dopo la ricezione e protocollazione i dati saranno inseriti in un contenitore chiuso riferito all'interessato e successivamente trattati da personale incaricato e custoditi in appositi contenitori chiusi.

Allegati

A – documenti di nomina per l'assegnazione di responsabilità e incarichi

B – lista degli incaricati di trattamento con strumenti elettronici

C – lista degli incaricati di trattamento senza l'ausilio di strumenti elettronici

D – lista degli incaricati con funzioni di amministratore di sistema interni

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 28 di 40 |

ALLEGATO A

**ATTO DI NOMINA DEL RESPONSABILE
CON FUNZIONI DI COORDINAMENTO**
- art 29 decreto legislativo 30 giugno 2003, n° 196 -

Il/la sottoscritt Sindaco del Comune di
....., in qualità di **titolare del trattamento dei dati personali** da esso
operato, ai sensi e per gli effetti del decreto legislativo 30 giugno 2003, n° 196, con il presente atto

**NOMINA
RESPONSABILE DEL TRATTAMENTO DEI DATI
CON FUNZIONI DI COORDINAMENTO**

Il/la Sig., nato/a a, il,
nella sua qualità di

- a) in quanto preposto al trattamento dei dati personali effettuato da questo Comune, in relazione alla funzione che le/gli è propria, riguardante in modo specifico il ... < *settore / area / servizio* >...;
- b) in relazione alla funzione di coordinamento tecnico di tutti i responsabili, interni ed esterni, collaborando con il titolare per la realizzazione degli adempimenti generali disposti dal D.Lgs. 30 giugno 2003, n° 196, quali:
- predisposizione delle nomine a responsabile e verifica annuale delle stesse;
 - definizione ed aggiornamento del Documento programmatico per la sicurezza;
 - verifiche periodiche sulla attivazione e sulla efficacia delle misure di sicurezza;
 - verifiche periodiche sull'operato dei responsabili;
 - tenuta del fascicolo riguardante gli atti previsti dal Codice;
 - nomina dell'incaricato con funzioni di amministratore di sistema;
 - controllo e verifica dell'attività dell'incaricato con funzioni di amministratore di sistema.

Il Sig., nella qualità di cui al precedente punto a), ha il potere di compiere tutto quanto necessario per il rispetto delle vigenti disposizioni. In particolare dovrà:

1. Operare perché il trattamento dei dati avvenga secondo le modalità definite dalla normativa in vigore;
2. Verificare che il trattamento dei dati avvenga in modo lecito;
3. Verificare che l'informativa all'interessato sia stata effettuata;
4. Operare per garantire l'effettivo esercizio dei diritti dell'interessato (art 7 Codice);
5. Rispettare e far rispettare le misure di sicurezza indicate dalla vigente normativa in materia di tutela dei dati personali e predisposte da questo Comune, nel proprio ambito di competenza;
6. Individuare gli incaricati di trattamento dando loro istruzioni scritte;
7. Interagire con il Garante, in caso di richieste di informazioni o effettuazione di controlli ed accessi da parte dell'Autorità;
8. Informare prontamente il titolare di ogni questione rilevante ai fini della legge;
9. predisporre un rapporto scritto in merito agli adempimenti eseguiti ai fini della legge ed alle conseguenti risultanze, con periodicità annuale;
10. Predisporre le risposte, non oltre le 24 ore successive al loro ricevimento, ai reclami degli interessati e le eventuali istanze al Garante;
11. Tenere, in riferimento alla propria/o ... < *settore / area / servizio* >... la lista degli incaricati e degli addetti alla gestione o manutenzione con l'indicazione dell'ambito di trattamento consentito con strumenti elettronici; aggiornare la lista almeno annualmente;
12. Provvedere all'assegnazione iniziale delle credenziali di autenticazione agli incaricati;

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 29 di 40 |

13. Organizzare la custodia delle copie delle credenziali definite dai singoli incaricati, garantendone la necessaria segretezza;
14. Tenere, in riferimento alla propria/o ... < settore / area / servizio >... la lista degli incaricati con l'indicazione dell'ambito di trattamento consentito senza l'ausilio di strumenti elettronici; aggiornare la lista almeno annualmente;
15. Provvedere, in riferimento alla propria/o ... < settore / area / servizio >... alla gestione delle chiavi che danno accesso ai locali (custodia delle copie, assegnazione agli incaricati etc.);
16. Provvedere alla gestione delle chiavi degli archivi che contengono dati personali;
17. Acquisire, quando il Comune si avvale di soggetti esterni per provvedere alla installazione di misure minime di sicurezza, una descrizione della misura stessa che espliciti l'intervento effettuato e/o lo strumento fornito e che ne attesti la conformità al Discipinare allegato al Codice;
18. Autorizzare l'accesso agli archivi contenenti dati sensibili e giudiziari;
19. Verificare che vi sia il consenso dell'interessato per il trattamento dei dati sensibili, se necessario.

Data

Il Titolare

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 30 di 40 |

ATTO DI NOMINA DEL RESPONSABILE
- art 29 decreto legislativo 30 giugno 2003, n° 196 -

Il/la sottoscritt Sindaco del Comune di
....., in qualità di **titolare del trattamento dei dati personali** da esso
operato, ai sensi e per gli effetti del decreto legislativo 30 giugno 2003, n° 196 , con il presente atto

**NOMINA
RESPONSABILE DEL TRATTAMENTO DEI DATI**

Il/la Sig., nato a, il
....., nella sua qualità di
in quanto preposto al trattamento dei dati personali effettuato da questa Istituzione, in relazione alla
funzione che le/gli è propria, riguardante in modo specifico il ... < settore / area / servizio >....

Il Sig., nella predetta qualità, ha il potere di compiere
tutto quanto necessario per il rispetto delle vigenti disposizioni.
In particolare dovrà:

1. Operare perché il trattamento dei dati avvenga secondo le modalità definite dalla normativa in vigore;
2. Verificare che il trattamento dei dati avvenga in modo lecito;
3. Verificare che l'informativa all'interessato sia stata effettuata;
4. Operare per garantire l'effettivo esercizio dei diritti dell'interessato (art. 7 Codice);
5. Rispettare e far rispettare le misure di sicurezza indicate dalla vigente normativa in materia di tutela dei dati personali e predisposte da questo Comune, nel proprio ambito di competenza;
6. Individuare gli incaricati di trattamento dando loro istruzioni scritte;
7. Interagire con il Garante, in caso di richieste di informazioni o effettuazione di controlli ed accessi da parte dell'Autorità;
8. Informare prontamente il titolare di ogni questione rilevante ai fini della legge;
9. Predisporre un rapporto scritto in merito agli adempimenti eseguiti ai fini della legge ed alle conseguenti risultanze, con periodicità annuale;
10. Predisporre le risposte, non oltre le 24 ore successive al loro ricevimento, ai reclami degli interessati e le eventuali istanze al Garante;
11. Tenere, in riferimento alla propria/o ... < settore / area / servizio >... la lista degli incaricati e degli addetti alla gestione o manutenzione con l'indicazione dell'ambito di trattamento consentito con strumenti elettronici; aggiornare la lista almeno annualmente;
12. Provvedere all'assegnazione iniziale delle credenziali di autenticazione agli incaricati;
13. Organizzare la custodia delle copie delle credenziali definite dai singoli incaricati, garantendone la necessaria segretezza;
14. Tenere, in riferimento alla propria/o ... < settore / area / servizio >... la lista degli incaricati con l'indicazione dell'ambito di trattamento consentito senza l'ausilio di strumento elettronici; aggiornare la lista almeno annualmente;
15. Provvedere, in riferimento alla propria/o ... < settore / area / servizio >... alla gestione delle chiavi che danno accesso ai locali (custodia delle copie, assegnazione agli incaricati etc.);
16. Provvedere alla gestione delle chiavi degli archivi che contengono dati personali;
17. Acquisire, quando il Comune si avvale di soggetti esterni per provvedere alla installazione di misure minime di sicurezza, una descrizione della misura stessa che espliciti l'intervento effettuato e/o lo strumento fornito e che ne attesti la conformità al Disciplinary allegato al Codice;
18. Autorizzare l'accesso agli archivi contenenti dati sensibili e giudiziari;
19. Verificare che vi sia il consenso dell'interessato per il trattamento dei dati sensibili, se necessario.

Data

Il Titolare

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 31 di 40 |

ATTO DI NOMINA DEL RESPONSABILE ESTERNO
- articolo 29 decreto legislativo 30 giugno 2003, n° 196 -

Il/la sottoscritt Sindaco del Comune di
....., in qualità di titolare del trattamento dei dati personali da esso
operato, ai sensi e per gli effetti del decreto legislativo 30 giugno 2003, n° 196 , con il presente atto

**NOMINA
RESPONSABILE DEL TRATTAMENTO DEI DATI**

la società/ditta ...<nome & ragione sociale>... legalmente rappresentata dal/dalla Sig.
.....

Tale nomina è in relazione alle operazioni di ...<elaborazione di dati personali>, <manutenzione>,
<pulizie>... ai quali il soggetto sopracitato ha accesso nell'espletamento delle attività previste dal
...<contratto/convenzione estremi atto>... fra lo stesso e il Comune di

In ottemperanza al D.Lgs. 30 giugno 2003, n° 196, che regola il trattamento dei dati personali, laddove costituisce trattamento "*qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione dei dati*", ed in relazione al presente atto di nomina la società/ditta ...<nome & ragione sociale>... nell'espletamento delle attività previste dal ...<contratto/convenzione estremi atto>... ha il potere di compiere tutto quanto necessario per il rispetto delle vigenti disposizioni.

In particolare dovrà:

1. rispettare le misure di sicurezza previste dalla legge e disposte dalla Amministrazione nel Documento programmatico per la sicurezza dei dati personali;
2. individuare gli incaricati, dando loro istruzioni scritte;
3. informare prontamente il Titolare di ogni questione rilevante ai fini della legge;
4. predisporre un rapporto scritto in merito agli adempimenti eseguiti ai fini della legge ed alle conseguenti risultanze con cadenza annuale o alla fine dell'attività;
5.<eventuali altre specifiche particolari>.....

Data

Il Titolare

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 32 di 40 |

ATTO DI NOMINA DEL RESPONSABILE ESTERNO
- articolo 29 decreto legislativo 30 giugno 2003, n° 196 -

Il/la sottoscritt Sindaco del Comune di
....., in qualità di **titolare del trattamento dei dati personali** da esso
operato, ai sensi e per gli effetti del decreto legislativo 30 giugno 2003, n° 196 , con il presente atto

**NOMINA
RESPONSABILE DEL TRATTAMENTO DEI DATI**

la società/ditta ...<nome & ragione sociale>... legalmente rappresentata dal/dalla Sig.
.....

Tale nomina è in relazione alle operazioni alle quali il soggetto sopracitato ha accesso
nell'espletamento delle attività previste dal ...<contratto/convenzione, estremi atto>... fra lo stesso e
il Comune di

In ottemperanza quanto disposto dal D.Lgs. 30 giugno 2003, n° 196, che regola il trattamento dei
dati personali, laddove costituisce trattamento "*qualunque operazione o complesso di operazioni
svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la
registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione,
l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la
cancellazione e la distribuzione dei dati*",

Alla luce di quanto disposto dal provvedimento generale del Garante per la protezione dei dati
personali del 27 novembre 2008 riguardante le attribuzioni delle funzioni di amministratore di
sistema.

In relazione al presente atto di nomina la società/ditta ...<nome & ragione sociale>...
nell'espletamento delle attività previste dal ...<contratto/convenzione estremi atto>... ha il potere di
compiere tutto quanto necessario per il rispetto delle vigenti disposizioni.

In particolare dovrà:

1. rispettare le misure di sicurezza previste dalla legge e disposte dalla Amministrazione nel Documento Programmatico per la Sicurezza dei dati;
2. individuare gli incaricati, dando loro istruzioni scritte;
3. informare prontamente il Titolare di ogni questione rilevante ai fini della legge;
4. predisporre un rapporto scritto in merito agli adempimenti eseguiti ai fini della legge ed alle conseguenti risultanze con cadenza annuale o alla fine dell'attività;
5. redigere e aggiornare un elenco con gli estremi identificativi delle persone fisiche preposte ad operare sul sistema informatico di questa Amministrazione, per provvedere ai servizi previsti dal ...<contratto/convenzione estremi atto>..., fornendole al Titolare qualora si renda necessario
6. ...<eventuali altre specifiche particolari>...

Data

Il Titolare

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 33 di 40 |

**ATTO DI NOMINA DELL'INCARICATO
CON FUNZIONI AMMINISTRATORE DI SISTEMA
- art 30 decreto legislativo 30 giugno 2003, n° 196 -**

Il sottoscritto, in qualità di ...<titolare>...<responsabile>... del trattamento dei dati personali da esso operato, ai sensi e per gli effetti del D.LGS 196/2003, e a seguito di previa valutazione della esperienza, capacità e affidabilità dimostrate (come da curriculum vitae allegato al fascicolo privacy), con il presente atto

**NOMINA INCARICATO
CON FUNZIONI AMMINISTRATORE DI SISTEMA**

il Sig. in qualità di

Tale nomina è in relazione alla gestione del sistema informatizzato della istituzione, secondo quanto disposto dal Disciplinare tecnico in materia di misure minime di sicurezza, allegato B al D.Lgs 196/2003, con i compiti di seguito specificati:

- ...<specificare nel dettaglio i compiti dell'amministratore di sistema>...

e dovrà essere esplicitata attenendosi alle seguenti modalità generali:

- operando alle dipendenze del<responsabile>.....<titolare>..... del trattamento dei dati ed eseguendo puntualmente le istruzioni dallo stesso impartite;
- rispettando durante le attività svolte le misure di sicurezza previste dalla legge e specificate nel Documento programmatico sulla sicurezza;
- garantendo la massima riservatezza nel trattamento dei dati;
- informando tempestivamente il ...<responsabile>...<titolare>... di anomalie nel funzionamento del sistema informatico che possano pregiudicare il corretto trattamento dei dati.

Le norme di comportamento dell'incaricato con funzioni di amministratore di sistema si esplicano:

- nel rispetto dei requisiti di diligenza professionale, richiesti dall'articolo 2050 del Codice Civile;
- nell'adeguamento preventivo ai contenuti espressi dal Titolo V Sicurezza dei dati e dei sistemi del D.Lgs 196/2003;
- nell'adozione di misure minime di cui all'allegato B al D.Lgs 196/2003, secondo quanto specificato nel Documento programmatico sulla sicurezza.

Data

Il Responsabile
con funzioni di coordinamento

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 34 di 40 |

ATTO DI NOMINA INCARICATO DEL TRATTAMENTO DATI
- art 30 decreto legislativo 30 giugno 2003, n° 196 -

Il/la sottoscritt in qualità di **responsabile del trattamento dei dati personali**, designato dal Sindaco del Comune di, ai sensi e per gli effetti del decreto legislativo 30 giugno 2003, n° 196, con il presente atto

**NOMINA
INCARICATO DEL TRATTAMENTO**

il/la Sig./a nella sua qualità di < *qualifica/funzione* >

Tale nomina è in relazione alle operazioni di elaborazione di dati personali ai quali il soggetto sopraccitato ha accesso nell'espletamento della funzione che le/gli è propria.
In ottemperanza al D.Lgs. 30 giugno 2003, n° 196, che regola il trattamento dei dati personali, laddove costituisce trattamento " *qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione dei dati*", ed in relazione al presente atto di nomina, è incaricato a trattare i dati personali (tutti quei dati idonei ad identificare direttamente o indirettamente una persona fisica o giuridica) attenendosi alle seguenti modalità:

1. In modo lecito e secondo correttezza;
2. Raccogliendoli e registrandoli per gli scopi inerenti l'attività svolta;
3. Verificando, ove possibile, che siano esatti e, se necessario, aggiornarli;
4. Verificando che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal responsabile;
5. Rispettando, nel trattamento, le misure di sicurezza previste dalle norme di legge e predisposte nell'Ente.
6. All'atto del ricevimento dei documenti (dati), effettuando le seguenti operazioni:
 - a) *non esporre i documenti (dati) a terzi;*
 - b) *procedere allo smistamento dei documenti in base alla tipologia degli stessi, non mettere in contatto i documenti di un interessato con quelli di un altro*
 - c) *custodire i documenti all'interno di contenitori riferiti all'interessato;*
 - d) *chiudere a chiave in apposito archivio i contenitori riferiti a dati sensibili;*
 - e) *nel caso in cui il soggetto interessato volesse consegnare dei dati in modo verbale, invitarlo a deporli in sede separata dove lo stesso incaricato procederà a verbalizzare quanto comunicato;*
7. Mantenere la rubrica telefonica, eventuali comunicazioni, documenti non alla portata di vista di chiunque abbia accesso all'ufficio.
8. All'atto del ricevimento dei documenti (dati) via fax, operando come segue:
 - a) *il fax deve essere situato in luogo non accessibile a soggetti diversi dagli incaricati;*
 - b) *inserire senza indugio il documento ricevuto in un contenitore riferito all'interessato e provvedere all'inoltro a chi di competenza;*
 - c) *verificare il documento nella sua leggibilità e se è il caso richiederne un rinvio.*
9. All'atto del ricevimento della posta, operando come segue:
 - a) *ritirare la posta personalmente e in via esclusiva;*
 - b) *lasciare le buste sigillate;*
 - c) *smistare la corrispondenza e trasmetterla a chi di competenza;*
 - d) *la corrispondenza non deve restare in vista di terzi;*
10. All'atto della consegna di documenti agli interessati, operando come segue:
 - a) *assicurarsi che il documento sia posto in un contenitore chiuso*

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 35 di 40 |

- b) assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in firma scritta.*
11. Alla luce di quanto sopra, in caso di allontanamento anche temporaneo dal posto di lavoro, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato.
 12. Nessun dato potrà essere comunicato a terzi o diffuso senza la preventiva specifica autorizzazione del titolare o responsabile ;
 13. I supporti cartacei contenenti dati personali riferiti agli interessati non necessari alle operazioni di trattamento (minute, appunti, telefax parzialmente illeggibili, etc) devono essere immediatamente distrutti.
 14. Nella gestione delle chiavi assumere i seguenti comportamenti:
 - a) conservare custodire con diligenza le chiavi affidate dal responsabile;*
 - b) avvertire tempestivamente il responsabile in caso di smarrimento o malfunzionamento delle chiavi;*
 - c) non fare copie delle chiavi affidate;*
 15. Nell'uso degli strumenti informatizzati per il trattamento assumere i seguenti comportamenti:
 - a) rispettare le indicazioni impartite dall'amministratore di sistema;*
 - b) non installare programmi dimostrativi o non certificati;*
 - c) non disinstallare programmi o eliminare file necessari al corretto uso e/o funzionamento della macchina;*
 - d) non modificare lo stato della macchina (hardware) di lavoro aggiungendo o eliminando periferiche;*
 - e) non rimuovere o rendere nulli i dispositivi di protezione installati sulla macchina: antivirus, password, ecc;*
 - f) rispettare la segretezza delle credenziali di autenticazione e delle password, modificare la password almeno una volta ogni 6 mesi, ogni tre mesi in caso del trattamento di dati sensibili e giudiziari;*
 - g) non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;*
 - h) custodire i supporti rimovibili (CD, floppy etc) su cui sono memorizzati dati sensibili e giudiziari in idonei contenitori provvisti di serratura;*
 - i) quando non più utilizzati i supporti rimovibili di cui al punto precedente devono essere distrutti o resi inintelligibili;*
 - j) operare in modo da garantire l'integrità e la disponibilità dei dati personali;*
 - k) provvedere al regolare svolgimento dei backup (salvataggio periodico dei dati), ove disposto, e secondo le norme prescritte dall'incaricato con funzioni di amministratore di sistema;*
 - l) limitare lo scambio di posta elettronica alle necessità dell'ufficio assumendo regole di buona condotta e atteggiamento consapevole nell'uso della posta elettronica;*
 - m) non effettuare la navigazione in Internet in siti controversi.*
 16. L'accesso agli archivi contenenti dati sensibili e giudiziari è autorizzato esclusivamente per l'espletamento della funzione che gli è propria, salvo casi particolari per i quali è necessaria specifica autorizzazione da parte del responsabile competente.

Data

Il Responsabile

| | | |
|-------------------------------|--|-------------------------------|
| Comune di Monte Argentario | D.P.S. | Revisione del Marzo 2010 |
| | <i>Documento Programmatico sulla Sicurezza dei dati</i> | Pagina 36 di 40 |

**ATTO DI NOMINA INCARICATO DEL TRATTAMENTO DATI
(PROFESSIONISTA ESTERNO)**

- art 30 decreto legislativo 30 giugno 2003, n° 196 -

Il/la sottoscritt in qualità di **responsabile del trattamento dei dati personali**, designato dal Sindaco del Comune di, ai sensi e per gli effetti del decreto legislativo 30 giugno 2003, n° 196, con il presente atto

**NOMINA
INCARICATO DEL TRATTAMENTO**

il/la Sig./a nella sua qualità di < *qualifica/funzione* >

Tale nomina è in relazione alle operazioni di elaborazione di dati personali ai quali il soggetto sopracitato ha accesso nell'espletamento della funzione che le/gli è propria e nello specifico riferita a < *specificare incarico* >

In ottemperanza al D.Lgs. 30 giugno 2003, n° 196, che regola il trattamento dei dati personali, laddove costituisce trattamento " *qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione dei dati*", ed in relazione al presente atto di nomina, è incaricato a trattare i dati personali (tutti quei dati idonei ad identificare direttamente o indirettamente una persona fisica o giuridica) attenendosi alle seguenti modalità:

17. In modo lecito e secondo correttezza;
18. Raccogliendoli e registrandoli per gli scopi inerenti l'attività svolta;
19. Verificando, ove possibile, che siano esatti e, se necessario, aggiornarli;
20. Verificando che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal responsabile;
21. Rispettando, nel trattamento, le misure di sicurezza previste dalle norme di legge e predisposte nell'Ente.
22. Nessun dato potrà essere comunicato a terzi o diffuso senza la preventiva specifica autorizzazione del titolare o responsabile ;
23. L'accesso agli archivi contenenti dati sensibili e giudiziari è autorizzato esclusivamente per l'espletamento dell'incarico in precedenza citato, salvo casi particolari per i quali è necessaria specifica autorizzazione da parte del responsabile competente.
24. < *altro specificare* >

Data

Il Responsabile

