



**COMUNE DI CITTA' DI CASTELLO**

**Provincia di Perugia**

**DISCIPLINARE TECNICO IN MATERIA DI MISURE  
MINIME DI SICUREZZA (Artt. da 33 a 36 del codice)**

**DECRETO LEGISLATIVO 196/2003  
(Allegato B)**

**DICEMBRE 2005**

# SOMMARIO

## TRATTAMENTO CON STRUMENTI ELETTRONICI

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato in caso di trattamento con strumenti elettronici

<b>1. SISTEMA DI AUTENTICAZIONE INFORMATICA.....</b>	<b>4</b>
1.1 STRUTTURA DEL SISTEMA E PROTEZIONI .....	4
1.1.1 Architettura della rete .....	4
1.1.2 Sicurezza della rete.....	4
1.1.3 Sicurezza dei dati.....	5
1.1.3.1 Banche dati centralizzate .....	5
1.1.3.2 Banche dati locali residenti su PC .....	6
1.1.4 Componenti del Sistema Informatico.....	7
1.2 PROFILI ORGANIZZATIVI E GESTIONALI .....	8
1.2.1 Incaricati del trattamento informatico .....	8
1.2.2 Soggetto preposto alla custodia delle password, alla loro attribuzione, cancellazione, modifica.....	8
1.2.3 Modalità di gestione delle password .....	8
<b>2. SISTEMA DI AUTORIZZAZIONE.....</b>	<b>10</b>
2.1 INDICAZIONI GENERALI .....	10
2.2 INDICAZIONI OPERATIVE .....	10
2.3 CUSTODIA DEI SUPPORTI RIMOVIBILI.....	10
<b>3. ALTRE MISURE DI SICUREZZA .....</b>	<b>10</b>
3.1 MISURE GENERALI .....	10
3.1.1 Salvataggio dei dati.....	10
3.1.2 Software antivirus.....	11
3.1.3 Interventi di accesso o manutenzione del PC.....	12
3.1.3.1 Richiesta di accesso .....	12
3.1.3.2 Interventi di manutenzione .....	12
3.1.4 Società esterne o professionisti che effettuano la manutenzione e l'assistenza .....	12
3.1.5 I locali.....	13
3.2 CAUTELE GENERALI PER IL PERSONALE PER I TRATTAMENTI CON STRUMENTI ELETTRONICI.....	13
3.2.1 Password .....	13
3.2.2 Uso del Personal Computer .....	14
3.2.3 Assenza dell'operatore .....	14
3.2.4 Uso e custodia dei supporti rimovibili.....	14
3.2.5 Quadro riepilogativo delle tipologie di banche dati e dei relativi codici.....	14
<b>4. ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI .....</b>	<b>15</b>
4.1 USO E CUSTODIA DEI SUPPORTI RIMOVIBILI.....	15
4.2 RIPRISTINO DEI DATI .....	15
<b>5. MISURE DI TUTELA E GARANZIA .....</b>	<b>15</b>
5.1 AGGIORNAMENTO DEL DPS.....	15

## TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato in caso di trattamento con strumenti diversi da quelli elettronici

<b>1. COMPITI DEL RESPONSABILE .....</b>	<b>16</b>
<b>2. COMPITI DELL'INCARICATO .....</b>	<b>16</b>
<b>3. QUADRO RIEPILOGATIVO DELLE MISURE MINIME PER IL TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI E RELATIVI CODICI.....</b>	<b>17</b>

## ALLEGATI

- A – LETTERA DI INCARICO AL RESPONSABILE**
- B – LETTERA DI INCARICO AGLI INCARICATI DEL TRATTAMENTO**
- C – LETTERA DI RESPONSABILITÀ DA PARTE DI PROFESSIONISTI O DITTE**
- D – DESIGNAZIONE DEL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI**
- E – CONSENSO AL TRATTAMENTO**
- F – INFORMATIVA**
- G – ESERCIZIO DEI DIRITTI**
- E – CONSENSO AL TRATTAMENTO**
- H – SCHEDA DI RILEVAZIONE DEL TRATTAMENTO DEI DATI**
- I – DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**

# **1. Sistema di autenticazione informatica**

## **1.1 Struttura del sistema e protezioni**

### *1.1.1 Architettura della rete*

Nel territorio comunale sono presenti sei sedi periferiche di cui quattro (Via XI Settembre, Via delle Giulianelle, Centro “Le Grazie”, Piazza Garibaldi) collegate alla sede principale tramite ponti radio Aironet a 2/4 Mbit/s, due (Via Sant’Antonio, Via della Montesca) collegate alla sede principale tramite fibra ottica. Sono presenti anche altre due sedi (Teatro Comunale, Magazzino) collegate alla sede principale tramite rete wireless con impiego di celle Navini e radio modem).

Sono collegati alla sede principale tramite modem su linee analogiche anche i quattro asili nido comunali (Franchetti, Fiocco di Neve, La Coccinella, Il Delfino), le tre farmacie comunali (Cerbara, Franchetti, Cinquemiglia), il Centro di aggregazione giovanile, il Centro di San Giovanni in Campo e l’Ufficio di Cittadinanza.

A breve questi collegamenti saranno sostituiti da collegamenti wireless.

La Delegazione di Trestina è collegata alla sede principale tramite router ISDN.

Sono collegati, inoltre, alla sede principale tramite modem su linee PSTN/ISDN la Sorit, la Polizia e tutti i soggetti preposti ad effettuare teleassistenza sulle procedure applicative.

Tutti i dipendenti dotati di PC sono quindi collegati alla rete Intranet attraverso la quale possono accedere alle varie applicazioni dell’Ente.

I dipendenti autorizzati all’accesso ad Internet vi accedono in un unico punto, filtrati dal sistema di firewall del Comune.

### *1.1.2 Sicurezza della rete*

La rete del Comune è connessa alla rete Internet mediante un firewall perimetrale 3Com Firewall SS3: inoltre il Comune è collegato agli altri enti pubblici tramite rete ComNet filtrata da un altro firewall ZYXEL ZYWALL35.

I collegamenti tra l’infrastruttura wireless e la rete comunale sono effettuati tramite VPN e filtrati attraverso il firewall ZYXEL ZYWALL35.

I quattro Asili Nido Comunali, le tre Farmacie Comunali, il Centro di aggregazione giovanile, il Centro di San Giovanni in Campo, l’Ufficio di Cittadinanza ed i soggetti preposti ad effettuare teleassistenza sulle procedure sono filtrati tramite un server di Remote Access 3Com RAS 1500.

Anche la Polizia accede alla banca dati demografica filtrata tramite lo stesso server di Remote Access 3Com RAS 1500.

La Sorit è collegata al server in cui sono residenti le banche dati della demografica tramite numero telefonico riservato e credenziali di accesso; entro la fine dell'anno la banca dati della demografica sarà duplicata in un altro server e tutti gli accessi da parte di Sorit, della Polizia e degli utenti interni autorizzati alla consultazione delle informazioni anagrafiche avranno accesso a questo server.

Gli utenti della rete sono collegati ad Internet tramite un server firewall Proxy che gestisce tutte le politiche di accesso verso l'esterno: il server in questione è un Windows Server 2003 + ISA Server 2004.

Quindi tutti gli accessi dalla Intranet ad Internet, e viceversa, sono filtrati dai firewall, che impediscono accessi indesiderati o non autorizzati.

Tutti i server pubblicati verso l'esterno (Server per la gestione del sito web e per la gestione della posta esterna, Server per la gestione del PRG e per la gestione delle informazioni relative alla Protezione Civile) e il proxy sono collegati ad una DMZ (Zone De Militarizzata), gestita dal firewall perimetrale 3Com Firewall SS3.

L'accesso di tutte le postazioni alla rete Intranet è effettuato tramite dominio Windows NT4 gestito da due server, uno principale ed uno di backup.

### *1.1.3 Sicurezza dei dati*

#### ***1.1.3.1 Banche dati centralizzate***

Le banche dati centralizzate sono residenti nei vari server presenti nella sala macchine del CED, nella sede principale del Comune.

Si riporta di seguito, nella tabella A, l'elenco delle banche dati centralizzate ed i nomi dei rispettivi server che le ospitano.

**Tabella A**

Nome Server	Sistema Operativo	Data Base	Banca Dati
Cast1	Unix	Informix	Aeraria (Contabilità prima di e-Serfin) CSIO (Stipendi prima di Zucchetti) Duplicazione Demos (Demografica)
Cast2	Unix	Informix	Demos (Demografica)
Flash	Windows NT4	Oracle	e-Serfin (Contabilità)

			e-Trib (Tributi) Concilia (Mulle) Tradewin (Commercio)
Urano	Windows 2000	Access	PRG (Consultazione in Internet del Piano Regolatore Generale) Azimut (Protezione Civile)
Hypnos	Windows 2000	Lotus Notes	Si.Ge.D (Protocollo, Delibere,Atti)
Argo	Windows 2003	SQL Server	Sosia (Ristorazione scolastica) Gradus (Graduatorie nidi) Zucchetti (Paghe)
			Programmi realizzati dal CED (____)

Sono presenti presso la sala macchine del CED altri server che riportiamo di seguito nella Tabella B solo per completezza di informazioni e perché saranno richiamati in altre parti del disciplinare.

**Tabella B**

Nome Server	Sistema Operativo	Banca Dati
NT1	Windows NT4	Dominio principale Posta interna Stampanti di rete
Intgw	Windows NT4	Dominio di backup Proxy Internet
Aracne	Windows 2000	Pubblicazione sito Posta esterna
Argo	Windows 2003	Application Server per le procedure che sono in Terminal Server
Nas1	Windows 2000 server	Backup Nas Server (Cartelle condivise)
Atena	Windows 2003 server	Gestione Antivirus Backup per procedure in SQL Server

La protezione delle banche dati residenti nei server della Intranet (server centralizzati e localizzati nella sala macchine del CED presso la sede centrale) si ottiene mediante l'uso di credenziali di autenticazione userid e password, che vengono assegnate e gestite dal CED: ogni singola applicazione protegge i propri dati dall'accesso non autorizzato mediante controllo di userid e password; tali userid e password sono individuali.

Al singolo dipendente, autorizzato all'accesso, possono essere assegnate più userid e password diverse tra loro a seconda dell'applicazione alla quale accede.

### ***1.1.3.2 Banche dati locali residenti su PC***

I PC che contengono banche dati locali, contenenti dati personali e/o sensibili, devono essere protetti da credenziale di accesso.

Per tutti i sistemi operativi presenti nei Personal Computer (Windows 95/98 Windows 2000 o successivi) la credenziale di accesso è costituita dalla combinazione di userid e password.

La password che viene assegnata dal CED al momento dell'assegnazione del Personal Computer può essere modificata dal dipendente al quale è affidato il PC.

Comunque la modifica della password è a carico del dipendente al quale è assegnato il PC: tale modifica deve essere effettuata nei tempi e nei modi previsti dalla legge (tre o sei mesi a seconda del tipo di dato).

Per gli account di Posta Esterna valgono le stesse regole relative alla gestione e modifica delle password: ogni tre o sei mesi a seconda del tipo di dato trattato deve essere modificata la password.

#### *1.1.4 Componenti del Sistema Informatico*

Il sistema di gestione delle banche dati è strutturato come di seguito riportato.

Le applicazioni gestionali principali sono residenti nei rispettivi server: tutte le banche dati sono protette da userid e password individuali assegnate; sono assegnate credenziali di accesso anche per gruppi omogenei di autorizzazione, quali ad esempio l'accesso alla banca dati della Demografica.

Le applicazioni gestionali secondarie sono residenti su singole postazioni che possono avere sistemi operativi vari: anche in questo caso i dati contenuti nei singoli PC sono protetti da userid e password individuali assegnate.

Gli archivi presenti nella Rete Civica, quali ad esempio la bacheca elettronica, sono residenti su server: anche in questo caso i dati contenuti sono protetti da userid e password individuali assegnate.

Il sistema di gestione della Posta interna ed esterna è strutturato come di seguito riportato.

La Posta elettronica interna è residente nello stesso server in cui vengono gestiti il dominio principale e le stampanti di rete: le caselle di posta elettronica interna sono individuali, nominative o di servizio, e sono protette da userid e password individuali e personali.

La Posta elettronica esterna è residente nello stesso server in cui viene gestita la pubblicazione del sito web (www.cdcnet.net) del Comune: le caselle di posta

elettronica esterna sono individuali, nominative per i Dirigenti di settore, di servizio per altri dipendenti. In entrambi i casi le caselle di posta elettronica esterna sono protette da userid e password individuali e personali.

Il sistema per la gestione del software Antivirus è residente nello stesso server dove avviene il salvataggio delle procedure realizzate in SQL Server.

Il sistema di gestione delle cartelle condivise risiede nel server Nas1: per ogni Settore e/o Servizio viene creata una cartella con tante sotto-cartelle quanti sono i soggetti o i gruppi di soggetti che devono accedere agli stessi dati. Tutte le cartelle e le relative sotto-cartelle vengono salvate giornalmente. I salvataggi di dette cartelle seguono lo stesso ciclo dei salvataggi delle banche dati che risiedono nei server della Tabella A.

Nel server Nas1 vengono salvate giornalmente anche le banche dati e-Serfin, e-Trib, Concilia, Tradewin, Si.GE.D., Sosia, Gradus, Zucchetti.

Le stampanti di rete sono gestite nel server dove sono gestiti il dominio principale e la Posta interna.

## **1.2 Profili organizzativi e gestionali**

### *1.2.1 Incaricati del trattamento informatico*

Sono incaricati del trattamento informatico dei dati, a seconda delle specifiche competenze, e per le banche dati centralizzate, tutti i dipendenti del CED.

### *1.2.2 Soggetto preposto alla custodia delle password, alla loro attribuzione, cancellazione, modifica*

Preposto alla gestione delle password per l'accesso alle banche dati centralizzate è il Dirigente del CED in qualità di Responsabile del trattamento dei dati relativi al proprio settore. Nell'ambito della designazione del personale incaricato, lo stesso provvederà alla designazione di un incaricato per la custodia, l'attribuzione, la cancellazione e la modifica delle password.

Le credenziali di accesso userid e password, per quanto riguarda le banche dati centralizzate ed i PC che accedono a cartelle personali o condivise residenti comunque nei server centralizzati, vengono assegnate e gestite dal personale del CED; è a cura di tale servizio comunicare la scadenza delle password.

Ogni tre o sei mesi a seconda del tipo di dato, infatti, il server di autenticazione non consentirà l'accesso se non agli utenti che abbiano modificato la password.

### *1.2.3 Modalità di gestione delle password*

Per le banche dati informatizzate centralizzate devono essere seguite le regole di seguito riportate:

- a. il responsabile delle singole banche dati, o il Dirigente di settore per le banche dati trasversali utilizzate dal suo settore (quali ad esempio la visualizzazione di alcuni dati della Demografica), deve prontamente comunicare eventuali cambi di mansione e dimissioni degli incaricati, nonché la nomina di nuovi incaricati, al soggetto preposto o al soggetto da questo incaricato
- b. il soggetto preposto o il soggetto da questo incaricato deve prontamente intervenire eliminando o aggiornando le credenziali di accesso utente e password in dotazione all'incaricato.

Per le banche dati residenti nei PC individuali il Dirigente di Settore, in qualità responsabile del trattamento dei dati, deve seguire le regole di seguito riportate:

- a. nel caso di dimissione di un dipendente deve prontamente avvisare il soggetto preposto, o il soggetto da questo incaricato, per la pulizia o recupero delle banche dati residenti nel PC prima della assegnazione dello stesso ad altro dipendente
- b. nel caso di trasferimento del dipendente ad altro servizio o settore, senza contemporaneo trasferimento del PC deve comportarsi come al punto a.
- c. nel caso di trasferimento del dipendente ad altro servizio o settore, con contemporaneo trasferimento del PC, deve avvisare il soggetto preposto, o il soggetto da questo incaricato, per la pulizia o il recupero delle banche dati residenti nel PC, di interesse del settore o servizio di provenienza.

Il soggetto preposto, o il soggetto da questo incaricato, deve prontamente intervenire eliminando o trasferendo le banche dati in dotazione all'incaricato.

Ogni incaricato che riceve le proprie password ne è direttamente responsabile e non deve in alcun modo comunicarle a persone diverse od altri incaricati; qualora avesse il timore che la propria password sia divenuta di conoscenza di altri soggetti deve prontamente darne comunicazione al responsabile preposto, o al soggetto da questo incaricato, al fine di attivare la procedura di sostituzione di cui sopra.

Il PC non deve essere lasciato acceso incustodito.

Il responsabile preposto alla gestione delle password, o il soggetto da questo incaricato, può variare le password degli incaricati, quando lo ritiene opportuno, dandone pronta comunicazione agli stessi in busta chiusa.

La password deve essere modificata ogni sei mesi; nel caso di trattamento di dati sensibili o giudiziari deve essere modificata ogni tre mesi.

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

## **2. Sistema di autorizzazione**

### **2.1 Indicazioni generali**

Per gli incaricati possono essere individuati profili di autorizzazione di ambito diverso. Ciò accade in modo particolare per incaricati che devono operare su banche dati trasversali quale ad esempio la banca dati Demografica. In tal caso i profili di autorizzazione che possono essere presenti per ciascun incaricato o per classi omogenee di incaricati, devono essere individuati e configurati prima del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

### **2.2 Indicazioni operative**

I singoli responsabili di settore chiederanno formalmente al responsabile del trattamento dei dati della specifica banca dati, l'accesso a determinate informazioni per determinati incaricati.

In base alla banca dati trattata il responsabile del trattamento della stessa comunicherà al CED, se la stessa è gestita da detto servizio, o alla ditta esterna che la gestisce, le informazioni e gli incaricati che ad esse devono accedere.

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione o la revoca dei profili di autorizzazione.

### **2.3 Custodia dei supporti rimovibili**

Devono essere impartite, da parte del responsabile del trattamento dei dati, le istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

## **3. Altre misure di sicurezza**

### **3.1 Misure generali**

#### *3.1.1 Salvataggio dei dati*

Il salvataggio delle banche dati centralizzate residenti nei server è in carico al CED, mentre ogni singolo incaricato è responsabile del salvataggio degli archivi residenti nel PC in cui opera, anche se questi sono condivisi con altri PC in rete.

Le banche dati residenti nei server vengono salvate quotidianamente allo scopo di fornire almeno una versione aggiornata alla notte precedente: le banche dati delle procedure e-Serfin, e-Trib, Concilia, Tradewin, Si.GE.D., Sosia, Gradus e Zucchetti vengono inoltre salvate anche nel server Nas1.

Le copie vengono effettuate su cassette a nastro magnetico ad alta capacità e riposte in una cassaforte ignifuga posta in altro locale distante dai locali del CED (locale Messi Comunali a piano terra).

Le copie giornaliere vengono ricoperte ogni quindici giorni, le mensili ogni 4 mesi: vengono conservate per tre anni le copie al 31.12 di ogni anno.

Prima di ogni aggiornamento delle procedure centralizzate a versioni successive viene effettuato un salvataggio ulteriore della procedura in questione che viene conservato per un mese.

Ogni lunedì o primo giorno utile della settimana viene controllato dall'incaricato dei salvataggi dei dati la correttezza degli stessi.

Le banche dati residenti soltanto nel singolo PC sono salvate in un supporto magnetico a disposizione del singolo dipendente (floppy, CD Rom, DVD).

Tempi e modalità del salvataggio dei dati trattati sono definiti nelle istruzioni impartite agli incaricati dai responsabili del trattamento dei dati e comunque con cadenza almeno settimanale.

### *3.1.2 Software antivirus*

Su tutti i PC è installato il programma antivirus che viene aggiornato automaticamente all'accensione tramite l'accesso in rete al server Atena che gestisce detto software; l'antivirus installato nei singoli PC controlla in tempo reale i documenti utilizzati.

Il sistema antivirus installato agisce sia a livello di PC che di server. Tutti i server sono dotati di detto software.

Il sistema filtra in modo sicuro i virus conosciuti secondo le modalità di seguito riportate:

- a. nel server di posta elettronica intervenendo in modo automatico per la ricerca di eventuali virus: una volta intercettato il virus, viene rifiutato il messaggio di posta e viene inviata una comunicazione elettronica a chi ha spedito la e-mail infetta

- b. nei singoli client intervenendo sia proteggendo la postazione a livello di rete locale, sia verso il collegamento ad Internet, sia nei confronti di supporti esterni quali floppy, CD-ROM e penne.

Il server che gestisce il software antivirus si aggiorna, automaticamente e quotidianamente, mediante collegamento via Internet al server dell'azienda produttrice.

Tutti i server ogni giorno eseguono il controllo degli aggiornamenti critici dei vari Sistemi Operativi che vengono installati automaticamente.

### *3.1.3 Interventi di accesso o manutenzione del PC*

#### **3.1.3.1 Richiesta di accesso**

Nel caso di prolungata assenza o impedimento del dipendente che renda indispensabile e indifferibile intervenire, per esclusiva necessità di operatività o sicurezza, nel PC in dotazione, il Dirigente responsabile di settore, in qualità di responsabile del trattamento dei dati, richiede ed autorizza l'intervento dei tecnici del CED, che ne permettono l'accesso per il tempo necessario.

Questo intervento verrà documentato e comunicato dal responsabile del CED al Dirigente del settore richiedente e, per conoscenza, al dipendente.

L'intervento dei tecnici del CED può avvenire accedendo con una password "di servizio" fino al rientro del dipendente, momento in cui allo stesso sarà riassegnata la sua password originale od altra.

Questa modalità di intervento consente ai singoli settori di non istituire il registro delle password individuali.

#### **3.1.3.2 Interventi di manutenzione**

Quando occorre effettuare in un PC un intervento di manutenzione, ordinaria o straordinaria, in loco o presso i locali del CED, sarà cura del dipendente concordare modi e tempi di intervento con i tecnici addetti.

Se l'intervento necessita dell'accesso al PC con le credenziali del dipendente, queste, se possibile, saranno inserite dallo stesso e non comunicate al tecnico.

Nel caso in cui il dipendente non possa presenziare all'intervento, questi comunicherà le proprie credenziali al tecnico e provvederà a modificarle una volta terminato l'intervento.

#### **3.1.4 Società esterne o professionisti che effettuano la manutenzione e l'assistenza**

Le società che effettuino assistenza e/o manutenzione dei sistemi hardware o software sono considerate responsabili del trattamento dei dati e devono, a tale scopo, rispettare le regole di seguito riportate:

- a) non effettuare copie né procedere alla eliminazione delle banche dati di titolarità del Comune
- b) informare preventivamente gli interessati del giorno e dell'orario in cui saranno effettuati gli interventi tecnici
- c) eventuali interventi remoti di assistenza mediante collegamento devono essere preventivamente autorizzati dai tecnici del CED che dovranno essere, altresì, avvisati al termine delle operazioni
- d) sottoscrivere un impegno formale al rispetto di tutte le norme e di tutte le indicazioni riportate nel presente documento
- e) usare riservatezza su dati ed informazioni addivenuti in loro possesso

### *3.1.5 I locali*

I locali del CED, a tutela della sala macchine dove risiedono i server, sono dotati di alcuni accorgimenti minimi, di seguito riportati, a garanzia sia della sicurezza fisica dell'hardware, sia delle banche dati:

- chiusura di sicurezza per la porta di ingresso ai locali del CED ed accesso controllato da citofono per tutti i soggetti non dipendenti del CED
- stabilizzatore di temperatura per la sala macchine
- gruppo di continuità e di stabilizzazione della corrente (su ogni gruppo di continuità sono appoggiati più server tenendo conto di un carico equilibrato)
- cassaforte ignifuga per cassette, floppy, CD Rom, DVD di salvataggio posta in luogo distante dai locali del CED (locali dei Messi Comunali a piano terra)
- presenza di un estintore all'ingresso dei locali del CED

## **3.2 Cautele generali per il personale per i trattamenti con strumenti elettronici**

### *3.2.1 Password*

Devono essere impartite, da parte del responsabile del trattamento, le istruzioni relative alle necessarie cautele al fine di assicurare la segretezza delle credenziali di autorizzazione: userid e password. La password deve essere composta da almeno otto caratteri.

Le password non devono contenere riferimenti agevolmente riconducibili all'incaricato e dopo il primo inserimento sono modificate successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili o di dati giudiziari la password

è modificata almeno ogni tre mesi.

### 3.2.2 *Uso del Personal Computer*

Il responsabile del trattamento dei dati deve impartire le opportune istruzioni per non lasciare incustodito e accessibile il PC durante una sessione di lavoro.

### 3.2.3 *Assenza dell'operatore*

Il responsabile del trattamento dei dati richiede ed autorizza l'intervento dei tecnici del CED, così come previsto al punto 3.1.3 ed assume le opportune misure per assicurare la disponibilità dei dati trattati con strumenti elettronici in caso di prolungata assenza o impedimento degli incaricati.

### 3.2.4 *Uso e custodia dei supporti rimovibili*

Il responsabile del trattamento dei dati deve impartire le indicazioni per l'uso, la custodia e l'eventuale distruzione dei supporti rimovibili, così come previsto ai punti 2.3 e 4.1.

### 3.2.5 *Quadro riepilogativo delle tipologie di banche dati e dei relativi codici*

Codice	Descrizione	Misure di Sicurezza	
		Tipologia	Responsabilità
1	Banca dati informatizzata , centralizzata	tecnica e organizzativa	CED
2	Banca dati residente su PC personale	tecnica e organizzativa	incaricato
3	Banca dati informatizzata, che utilizza il sistema di cifratura per proteggere i dati sensibili o giudiziari	tecnica e organizzativa	CED
4	Banca dati residente su supporti di memorizzazione non in linea (CD ROM, DVD, Floppy)	tecnica e organizzativa	incaricato

Le schede di rilevazione dei trattamenti dei dati (Allegato H) dovranno fare riferimento ai codici sopra evidenziati. Qualora per un particolare trattamento i codici siano più di uno, vanno indicati tutti.

## **4. Ulteriori misure in caso di trattamento di dati sensibili o giudiziari**

### **4.1 Uso e custodia dei supporti rimovibili**

Devono essere impartite, da parte del responsabile del trattamento dei dati, le istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati.

Le copie di backup effettuate sia dal personale tecnico del CED per le banche dati centralizzate sia dai singoli utenti per le banche dati residenti nei relativi PC, indipendentemente dai supporti impiegati, in ogni caso, quando tali supporti non sono più utilizzati, possono essere archiviati o distrutti, ma non utilizzati per archiviare altre tipologie di dati o per trasmetterli all'esterno.

I PC obsoleti, non più utilizzabili, vengono resi inservibili ed i loro dischi magnetici illeggibili prima della rottamazione; i dischi dei PC usati che il Comune decidesse di cedere in comodato d'uso gratuito prima della consegna vengono riformattati, impedendo l'accesso alle banche dati che vi erano contenute.

### **4.2 Ripristino dei dati**

Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi e compatibili con i diritti degli interessati e comunque non superiore a sette giorni.

Il responsabile del trattamento dei dati richiede, al CED o a ditta esterna, in base a chi ha sviluppato il software per la gestione della banca dati, indicazioni scritte circa le modalità di ripristino della stessa.

## **5. Misure di tutela e garanzia**

### **5.1 Aggiornamento del DPS**

Il Titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del Documento Programmatico sulla Sicurezza.

## TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato in caso di trattamento con strumenti diversi da quelli elettronici

Il trattamento "cartaceo" di dati personali deve essere garantito da particolari misure minime di sicurezza che devono essere specificate dal singolo responsabile del trattamento dei dati nelle istruzioni impartite agli incaricati per le diverse tipologie di trattamento.

### **1. Compiti del responsabile**

In particolare il responsabile del trattamento dei dati deve:

- coordinare tutte le operazioni di trattamento dei dati e vigilare sull'osservanza delle istruzioni impartite;
- curare l'informazione agli interessati relativa al trattamento dei dati e alla loro comunicazione;
- assegnare agli incaricati del trattamento le istruzioni per la corretta raccolta, elaborazione, consultazione e custodia dei dati;
- rettificare i dati su richiesta dell'interessato o d'ufficio, quando necessario;
- impartire le disposizioni operative per la sicurezza dell'accesso ai dati e ai documenti;
- curare l'eventuale relazione tra il trattamento effettuato e le singole banche dati gestite dal CED
- formulare proposte per l'eventuale distruzione, se consentito dalle norme, dei documenti contenenti dati non più necessari.

### **2. Compiti dell'incaricato**

In particolare l'incaricato del trattamento dei dati deve:

- trattare i dati esclusivamente per gli scopi definiti dall'ambito di trattamento assegnato. I dati non possono in alcun modo essere comunicati a terzi non incaricati

- osservare le norme di diligenza, prudenza e cautela per prevenire lo smarrimento, la distruzione o la perdita di documenti contenenti dati personali e per prevenire l'accesso o il trattamento da parte di persone non autorizzate
- assicurare la custodia delle chiavi di locali, armadi e cassettiere in cui sono conservati i documenti contenenti dati sensibili o giudiziari e, in caso di furto o smarrimento, deve essere fatta pronta denuncia al responsabile del trattamento dei dati
- in caso di assenza dall'ufficio, per cui il medesimo risulta non presidiato, i singoli documenti temporaneamente estratti dall'archivio per motivi di lavoro devono essere protetti in luogo custodito e non possono essere lasciati sulle scrivanie o alla libera visione di terzi
- si deve evitare di effettuare il trattamento dei dati personali in presenza di terzi che possano così venire a conoscenza, anche occasionalmente, dei dati
- nel caso in cui accedano agli archivi persone, a qualunque titolo, dopo l'orario di chiusura, devono essere preventivamente autorizzate e registrate

### **3. Quadro riepilogativo delle misure minime per il trattamento senza l'ausilio di strumenti elettronici e relativi codici**

Codice	Descrizione	Misure	
		Tipologia	Responsabili
5	Locali muniti di sicurezza (chiusi a chiave in caso di assenza dell'incaricato)	Organizzativa	incaricati
6	Archivi/contenitori muniti di sicurezza (chiusi a chiave in caso di assenza dell'incaricato)	Organizzativa	incaricati
7	Autorizzazione agli accessi fuori orario	Organizzativa	Dirigente responsabile
8	Rilascio autorizzazione formale agli incaricati con le istruzioni per tutti gli operatori	Organizzativa	Dirigente responsabile

Le schede di rilevazione dei trattamenti dei dati (Allegato H) dovranno fare riferimento ai codici sopra evidenziati. Qualora per un particolare trattamento i codici siano più di uno, vanno indicati tutti.