

Comune di Modena

**DISCIPLINARE TECNICO IN MATERIA DI MISURE  
MINIME DI SICUREZZA**

DECRETO LEGISLATIVO 196/2003

(allegato B)

approvato con delibera della Giunta Comunale n.164 del 30/3/2011

## SOMMARIO:

### A) Trattamento dei dati con strumenti elettronici

#### 1) Struttura del sistema e protezioni

*1.1 Architettura della rete*

*1.2 Sicurezza della rete*

*1.3 Architettura del Sistema Informatico*

*1.4 Sicurezza dei dati*

#### 2) Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni

*2.1 Incaricati del trattamento informatico*

*2.2 Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica*

*2.3 Trattamento dei dati personali affidati ai lavoratori*

*2.4 Trattamento dei dati personali affidati a soggetti esterni*

*2.5 Modalità di gestione delle password*

*2.6 Disattivazione credenziali per disuso*

#### 3) Modalità di gestione delle stazioni di lavoro

*3.1 Soggetto preposto alla pulizia o recupero delle banche dati su PC*

*3.2 Programma antivirus*

*3.3 Interventi di accesso e manutenzione del PC*

*3.4 Società esterne o professionisti per la manutenzione e l'assistenza*

*3.5 Dismissione delle stazioni di lavoro*

#### 4) Salvataggio dei dati

#### 5) Locali

6) Cautele generali

6.1 *Password*

6.2 *Uso del computer*

6.3 *Custodia dei supporti*

7) Quadro riepilogativo delle banche dati e dei relativi codici

B) Documento programmatico sulla sicurezza .

C) Trattamento dei dati senza l'ausilio di strumenti elettronici.

1) Quadro riepilogativo delle misure di sicurezza tecniche per i trattamenti senza strumenti elettronici e dei relativi codici.

Allegati:

“A1” - Designazione responsabile esterno del trattamento.

“ A2” - Nomina incaricato al trattamento dei dati ( soggetti esterni )

“B”- Scheda rilevazione trattamento dati personali da allegare alla determinazione del Dirigente

“ C “ - Convenzione per l'accesso in consultazione alla banca dati informatizzata dell'anagrafe del Comune di Modena e per l'eventuale trasmissione in fruizione dei dati anagrafici

## **A) Il Trattamento dei dati con strumenti elettronici**

### **1) Struttura del sistema e protezioni**

#### ***1.1 Architettura della rete***

Sul territorio comunale ci sono quattro sedi, definite nodi principali, collegate tra di loro in fibra ottica, (ad un Gbit/sec) a formare un anello, alle quali sono collegate tutte le altre sedi definite nodi secondari; l'architettura ad anello permette il funzionamento della rete anche nel caso di guasto su una fibra di collegamento.

Tutte le Sedi comunali (oltre 50), ed alcuni servizi sul territorio gestiti dal Comune (es. il sistema di telecamere di video sorveglianza), sono collegati alla rete descritta in fibra ottica e con linee HDSL ed ISDN.

Tutti i dipendenti dotati di PC sono quindi collegati alla rete Intranet, dalla quale possono accedere alle applicazioni dell'Ente; i dipendenti autorizzati accedono ad Internet in un unico punto, filtrati dal sistema di firewall aziendale.

#### ***1.2 Sicurezza della rete***

La rete del Comune è connessa all'esterno attraverso diversi canali di trasmissione dati:

- Collegamento alle rete Lepida: questo è un collegamento internet, fornito da una società pubblica, attraverso il quale si realizza anche l'accesso alla RUPA.
- Collegamento a un internet provider privato, utilizzato in parallelo e come backup al collegamento Lepida
- Collegamenti su linea telefonica, tramite un access server
- Collegamenti GPRS/UMTS, tramite un accesso (APN) dedicato.

Attraverso i collegamenti internet è inoltre stato realizzato un sistema di VPN basato su software open source.

Sia quest'ultimo che i collegamenti tramite linea telefonica e APN dedicato, consentono l'accesso alla rete comunale tramite autenticazione con nome utente e password.

Tutti i sistemi elencati afferiscono a un sistema di firewall, che controlla il traffico dati in base a politiche di sicurezza prestabilite.

### *1.3 Architettura del Sistema Informatico*

#### *Banche dati*

I dati strutturati delle applicazioni gestionali possono essere memorizzati in:

- banche dati centralizzate, per le applicazioni utilizzate da più utenti
- più raramente, su stazione di lavoro per applicazioni mono-utente

Oltre alle banche dati delle applicazioni gestionali esistono archivi documentali non strutturati, residenti su :

- server centrali (file server)
- sulle stazioni di lavoro

#### *Posta elettronica*

La posta elettronica viene gestita internamente; ad ogni dipendente è assegnata una casella individuale; inoltre esistono caselle non nominali corrispondenti a gruppi di lavoro o figure istituzionali.

#### *Sistemi di autenticazione*

Attualmente sono presenti 2 sistemi centralizzati di autenticazione/autorizzazione:

- Directory server LDAP ( Lightweight Directory Access ), utilizzato per autenticare gli utenti di applicativi su ambienti Unix:
  - posta elettronica
  - navigazione internet
  - accessi via modem o VPN
  - applicativi su server web
- Dominio Windows Active Directory utilizzato per autenticare gli utenti di risorse condivise su rete come:
  - cartelle
  - stampanti

LDAP è l'archivio principale in cui sono memorizzate le informazioni personali e le autorizzazioni all'utilizzo delle procedure applicative.

Sono stati messi a punto meccanismi di aggiornamento e allineamento degli utenti fra i vari sistemi.

- I dati personali degli utenti dipendenti del Comune di Modena presenti su LDAP vengono aggiornati automaticamente estraendoli dagli archivi del Settore Personale
- Le modifiche alla password su LDAP vengono riportate automaticamente sul dominio Active Directory

Alcune procedure applicative non utilizzano questi sistemi centralizzati, ma possiedono un proprio sistema di autenticazione ed autorizzazione degli utenti.

Per l'accesso ai personal computer non ci si avvale dei sistemi precedentemente citati, ma solo di credenziali locali.

Nei personal computer con sistema Windows 2000 e seguenti, è stato utilizzato il sistema nativo di autenticazione tramite username e password definite come credenziali locali, cioè memorizzate sul PC stesso .

Ad ogni singolo utente possono essere assegnate più credenziali, diverse fra loro, a seconda delle procedure applicative alle quali accede.

#### ***1.4 Sicurezza dei dati***

##### *Banche dati centralizzate*

L'accesso ai dati avviene tramite le procedure gestionali che li trattano: all'utente viene richiesta la digitazione di username e password. Queste credenziali sono verificate dalla procedura stessa.

Contestualmente viene verificato se l'utente è autorizzato all'utilizzo della funzionalità richiesta.

### *Archivi documentali centralizzati*

I server contenenti archivi documentali richiedono l'autenticazione e l'autorizzazione dell'utente tramite il dominio Active Directory.

Questa autenticazione avviene in modo trasparente per l'utente (senza la richiesta di ulteriore autenticazioni) se le credenziali di accesso al PC sono le stesse che nel dominio Active Directory.

### *Banche dati ed archivi documentali residenti su P.C.*

I PC che contengono banche dati locali o archivi documentali, contenenti dati personali e/o sensibili, sono protetti da credenziali di accesso personali, come precedentemente descritto.

## **2) Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni**

### ***2.1 Incaricati del trattamento informatico***

Sono tutti gli operatori tecnici del Servizio Progetti Telematici e dell'Ufficio Sistema e Reti.

### ***2.2 Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica***

Preposto alla gestione delle credenziali per l'accesso alle banche dati centralizzate è il Responsabile dell'Ufficio Sistema e Reti del Settore Sistemi Informativi e Servizi Demografici del Comune, che provvederà alla designazione del personale incaricato.

Il preposto alla gestione delle credenziali provvede, ogni sei mesi, a fornire ad ogni Dirigente di Settore l'elenco aggiornato di tutti coloro che, a qualsiasi titolo, sono autorizzati ad accedere alle banche dati di quel Settore .

Il preposto alla gestione delle credenziali può variare la password degli incaricati, in caso che si renda indispensabile ed indifferibile , per esclusiva necessità di operatività e sicurezza del sistema, dandone pronta comunicazione agli stessi in modo riservato.

Nessuna responsabilità può essere addebitata al preposto alla gestione delle credenziali per eventuali ritardi od omissioni a lui non imputabili nella

concessione, revoca o modifica delle autorizzazioni.

### ***2.3 Trattamento dei dati personali affidati ai lavoratori***

#### *A) Assegnazione delle credenziali di autenticazione*

Le credenziali di autenticazione consistono in un codice per l'autenticazione dell'incaricato ( userid ) associato ad una parola chiave riservata( password ).

In caso di assunzione di un nuovo lavoratore, quest'ultimo, il Dirigente del Settore competente o il responsabile del trattamento dei dati da lui delegato richiede al preposto alla gestione l'assegnazione della casella di posta elettronica e delle credenziali di autenticazione. Il preposto alla gestione provvede all'assegnazione della posta elettronica, di userid e della password provvisoria inserendo le credenziali nella directory LDAP e comunica le credenziali all'utente in modo riservato. E' a cura del lavoratore sostituire la password provvisoria con quella definitiva.

Può accadere che, per esigenze di servizio, esistano credenziali d'accesso non legate ad un singolo lavoratore e che possono essere condivise da tutto un gruppo di operatori. Queste credenziali non possono consentire l'accesso a banche dati o documenti contenenti dati personali.

#### *B) Assegnazione delle autorizzazioni*

Per poter accedere, a qualsiasi titolo, alle applicazioni ed alle banche dati del Comune occorre essere autorizzati.

L'autorizzazione del singolo lavoratore ad accedere alle banche dati del Comune deve essere sempre preceduta dal conferimento dell'incarico al trattamento dei dati da parte del responsabile del trattamento dei dati d'intesa con il titolare del trattamento , vale a dire il Dirigente del Settore.

La competenza alla richiesta, revoca, modifica delle autorizzazioni è del Dirigente del Settore di appartenenza del lavoratore il quale può delegarla per iscritto al responsabile al trattamento dei dati .

#### Accesso ad applicazioni e banche dati del Settore di appartenenza

Il Dirigente del Settore di appartenenza/ responsabile delegato sulla base dell'incarico conferito al lavoratore, comunica per iscritto, anche via e.mail, al preposto alla gestione delle credenziali a quali banche dati il lavoratore è

autorizzato ad accedere. Il preposto alla gestione delle credenziali abilita il lavoratore alle banche dati di sua competenza e provvede a inoltrare la richiesta ai responsabili applicativi per le relative autorizzazioni

#### Accesso ad applicazioni e banche dati di altri Settori.

Nel caso che il lavoratore necessiti di accedere a banche dati di un altro Settore, l'incarico dovrà essere dato congiuntamente dal Dirigente del Settore di appartenenza e dal Dirigente di Settore titolare della banca dati utilizzata.

Una volta conferito l'incarico, il Dirigente del Settore di appartenenza/responsabile delegato richiede per iscritto, anche via e.mail, al preposto alla gestione l'abilitazione del lavoratore alle banche richieste, attestando che il Dirigente del Settore titolare della banca dati ne è stato informato

Il preposto alla gestione procede con le modalità indicate al paragrafo precedente .

#### Cessazione del rapporto di lavoro

Nel caso di cessazione del rapporto lavorativo, il preposto alla gestione delle credenziali, attraverso una procedura automatica, ricava dalla Banca dati centralizzata del Settore Personale il nominativo del lavoratore cessato, ne revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica, e ne informa, per iscritto, anche via e.mail, il responsabile informatico dell'applicazione.

Nel caso di rapporto di collaborazione coordinata e continuativa, di prestazione occasionale, di tirocinio formativo ed in genere in tutti i casi in cui non è possibile ricavare l'informazione dell'avvenuta cessazione in modo automatico dalla Banca dati centralizzata del Settore Personale, spetta al Dirigente del Settore competente/ responsabile delegato comunicare tempestivamente per iscritto, anche via e.mail, al preposto alla gestione delle credenziali l'avvenuta cessazione del rapporto di lavoro e chiedere la revoca delle relative credenziali e autorizzazioni. Il preposto alla gestione delle credenziali revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica e ne informa per iscritto, anche via e.mail, il Dirigente del Settore competente e il responsabile informatico dell'applicazione.

Prima della cessazione del rapporto di lavoro, il lavoratore deve eliminare dal suo PC i documenti e le e-mail che non siano di interesse del Settore, autorizzando per iscritto il Dirigente ad accedere ai documenti ed alle e-mail rimanenti. Il Dirigente di Settore/ responsabile delegato deve prontamente avvisare il soggetto preposto alla pulizia o recupero delle banche dati di cui al punto 3.1 che provvederà al ritiro della stazione di lavoro o comunque a rendere indisponibili i dati legati al profilo del lavoratore dopo averne

trattenuto una copia. Entro un mese il Dirigente di Settore/ responsabile delegato può richiedere il recupero delle banche dati e delle e.mail giacenti nella casella di posta disabilitata, esibendo la relativa autorizzazione del lavoratore. Trascorso tale periodo il preposto provvederà alla eliminazione definitiva dei suddetti dati.

### Trasferimento del lavoratore

Nel caso di trasferimento presso un altro Settore di un lavoratore, il preposto alla gestione delle credenziali, dopo aver rilevato l'informazione attraverso la Banca dati centralizzata del Settore Personale, provvede a revocare tutte le autorizzazioni all'accesso del lavoratore, ad eccezione dell'indirizzo di posta elettronica, e ne informa per iscritto, anche via e.mail, il responsabile informatico dell'applicazione. Il lavoratore trasferito deve reindirizzare al Settore di provenienza tutta la corrispondenza di posta elettronica di competenza di quest'ultimo.

Il Dirigente del Settore di nuova assegnazione/ responsabile delegato , sulla base del nuovo incarico al trattamento dei dati conferito al lavoratore e delle competenze a quest'ultimo attribuite, provvede a richiedere le nuove abilitazioni, anche relative all'accesso a banche dati di un altro Settore, con le stesse modalità previste nel caso di nuova assunzione.

Nel caso di trasferimento di un lavoratore nell'ambito dello stesso Settore, il Dirigente di Settore/ responsabile delegato, sulla base del nuovo incarico al trattamento dei dati conferito al lavoratore e delle competenze a quest'ultimo attribuite, comunica per iscritto, anche via e.mail, al preposto alla gestione delle credenziali le autorizzazioni all'accesso da revocare e le nuove applicazioni, anche relative all'accesso a banche dati di un altro Settore, alle quali il lavoratore è autorizzato ad accedere. Il preposto alla gestione delle credenziali disabilita le autorizzazioni all'accesso da revocare, e per le nuove abilitazioni procede con le modalità previste nel caso di nuova assunzione informandone per iscritto, anche via e.mail, il Dirigente di Settore e il responsabile informatico dell'applicazione.

Nel caso che il trasferimento del lavoratore ( ad un altro Settore o nell'ambito dello stesso Settore ) comporti il contemporaneo trasferimento del PC, il lavoratore è tenuto a consegnare al Dirigente i dati e le e-mail di interesse del Settore e successivamente a rimuoverli dalla propria stazione di lavoro.

Nel caso invece in cui il trasferimento non comporti il contemporaneo trasferimento del PC, si deve seguire il comportamento previsto per il caso di cessazione del rapporto di lavoro

## ***2.4 Trattamento dei dati personali affidati a soggetti esterni***

Sono considerati soggetti esterni tutti quei soggetti che non rientrano nel punto 2.3 ( a puro titolo esemplificativo: società, enti, consorzi, professionisti , soggetti pubblici o gestori di pubblici servizi ).

La titolarità del trattamento dei dati resta in capo al Comune .

Il Dirigente del Settore contraente nomina il soggetto esterno responsabile del trattamento dei dati secondo l'allegato modello A1).

Nel caso in cui l'oggetto del contratto o della convenzione comporti l'utilizzazione di applicazioni o banche dati di competenza di più Settori, la designazione del responsabile dovrà essere sottoscritta congiuntamente dal Dirigente del Settore contraente e dai Dirigenti delle banche dati interessate. All'inizio della collaborazione il soggetto esterno responsabile del trattamento fornisce al Dirigente del Settore l'elenco degli incaricati al trattamento dei dati da lui nominati. Il Dirigente di Settore/ responsabile delegato , comunica per iscritto, anche via e.mail, al preposto alla gestione delle credenziali:

- a quali applicazioni l'incaricato è abilitato, richiedendo altresì, se necessario, l'accesso ad Internet e l'utilizzo della posta elettronica;
- la data di scadenza del contratto/ convenzione, se in suo possesso.

Nel caso in cui l'abilitazione riguardi banche dati di competenza di più Settori, nella comunicazione il Dirigente del Settore contraente dovrà altresì dare atto che i Dirigenti dei Settori interessati sono stati informati della richiesta.

Il preposto alla gestione delle credenziali imposta per l'utente un periodo massimo di validità delle credenziali di dodici mesi ( o inferiore se la data di scadenza del contratto/ convenzione è antecedente a tale termine). Scaduto il periodo di validità, le credenziali dell'utente, se non intervengono ulteriori comunicazioni, saranno automaticamente disabilitate. Qualora il contratto/ convenzione abbia una durata superiore all'anno, il responsabile esterno del trattamento dei dati, al fine di evitare che le credenziali degli incaricati siano automaticamente disabilitate alla scadenza dei dodici mesi, dovrà fornire al Dirigente di Settore, due mesi prima della scadenza delle stesse, l'elenco aggiornato degli incaricati. Il Dirigente di Settore/ responsabile delegato , trasmetterà al preposto alla gestione delle credenziali il nuovo elenco in sostituzione di quello precedente, comunicando, nel caso che nell'elenco siano presenti anche nuovi incaricati, le applicazioni a cui questi ultimi sono abilitati e richiedendo, se necessario, l'accesso ad Internet e

l'utilizzo della posta elettronica.

#### Accesso alla banca dati anagrafica

L'accesso alla banca dati anagrafica è consentito alle amministrazioni pubbliche e ai soggetti gestori o concessionari di servizi pubblici esclusivamente per finalità istituzionali.

L'accesso dovrà avvenire secondo le modalità e nei limiti specificati nella convenzione di cui all'allegato " C " che dovrà essere sottoscritta dal Dirigente del Settore Sistemi Informativi e Servizi Demografici e dal rappresentante della pubblica amministrazione / gestore o concessionario di servizi pubblici.

#### 2.5 Modalità di gestione delle password

Le password utilizzate nei sistemi di autenticazione LDAP e Active Directory sono assegnate dal preposto alla gestione delle credenziali all'atto della creazione delle credenziali stesse e vengono comunicate in forma riservata all'utente che deve provvedere, al primo utilizzo, alla sostituzione della password assegnata con una conosciuta solo dal medesimo.

La modifica della password LDAP comporta la modifica automatica anche della password Active Directory.

Su ogni nuova stazione di lavoro assegnata viene creato un profilo con lo stesso userid che l'utente ha sui sistemi centralizzati di autenticazione ma senza password. Il dipendente ha l'obbligo di impostare una password a propria scelta nel rispetto della normativa vigente.

Nei sistemi LDAP e Active Directory è stato impostato un meccanismo automatico di scadenza delle password ogni tre mesi. All'approssimarsi della scadenza l'utente LDAP viene avvertito via e.mail

Per motivazioni tecniche è opportuno avere un'unica password per l'accensione del PC, per l'accesso ad internet e per l'apertura della posta elettronica.

Il lavoratore, qualora dimentichi la password d'accesso al proprio PC, dovrà rivolgersi al lavoratore da lui delegato alla custodia delle password ( si veda paragrafo 3.3 ) o, in alternativa, al servizio di assistenza che si recherà sul posto e consentirà all'utente l'accesso al PC allo scopo di impostare una nuova password.

Qualora invece l'utente LDAP dimentichi la propria password, dovrà rivolgersi al lavoratore da lui delegato ( si veda paragrafo 3.3 ) o, in alternativa, all'Ufficio Sistema e Reti che provvederà, previa identificazione personale, a fornire in busta chiusa una password provvisoria che consentirà

di accedere alla procedura di modifica della password ma che dovrà poi essere immediatamente sostituita da una definitiva .

Qualora l'utente sia stato disabilitato per mancato uso delle credenziali per un periodo di almeno sei mesi, la procedura di riattivazione delle credenziali è quella di cui al successivo punto 2.6

Un utente che non sia stato disabilitato può, in qualsiasi momento, modificare la propria password LDAP autenticandosi con userid e vecchia password ( valida **solo** per questa funzione anche se scaduta ): la nuova password verrà scelta dall'utente tra quelle proposte dal sistema .

Ogni incaricato che riceve le proprie password ne è direttamente responsabile. Fatta eccezione per quanto previsto dal paragrafo 3.3, il lavoratore non deve in alcun modo comunicare le proprie password a persone diverse od altri incaricati; qualora avesse il timore che la propria password sia divenuta di conoscenza di altri soggetti deve prontamente provvedere a modificarla.

### ***2.6 Disattivazione credenziali per disuso.***

Il mancato uso delle credenziali per almeno sei mesi continuativi determina la loro disattivazione

Il Dirigente di Settore / responsabile delegato o, qualora ritenga di dover riattivare nuovamente le credenziali dell'utente, dovrà chiedere per iscritto, anche via e.mail, al preposto alla gestione delle credenziali il ripristino delle stesse.

L'utente dovrà rivolgersi all'Ufficio Sistema e Reti che provvederà, previa identificazione personale, a fornire in busta chiusa una password provvisoria che consentirà di accedere alla procedura di modifica della password ma che dovrà poi essere immediatamente sostituita da una definitiva .

## **3 ) Modalità di gestione delle stazioni di lavoro**

### ***3.1 Soggetto preposto alla pulizia o recupero delle banche dati su PC***

Preposto alla pulizia o recupero delle banche dati su PC è il Responsabile dell'Ufficio Sistema e Reti del Settore Sistemi Informativi e Servizi Demografici del Comune, che provvederà alla designazione del personale

incaricato.

### ***3.2 Programmi antivirus***

Su tutti i PC sono installati programmi antivirus che vengono aggiornati periodicamente in modo automatico, tramite l'accesso in rete al Server di gestione antivirus; l'antivirus installato sui singoli PC controlla in tempo reale i documenti utilizzati.

Oltre che sulle stazioni di lavoro sono installati sistemi antivirus sui server di posta elettronica, proxy per filtrare la navigazione, e file server, ovvero server che permettono la condivisione di documenti.

I Server di Gestione Antivirus si aggiornano in modo automatico

E' opportuno che l'utente, con periodicità almeno quindicinale, effettui con il software antivirus una scansione completa dei dischi interni della stazione di lavoro.

### ***3. 3 Interventi di accesso o manutenzione del PC***

#### *Richiesta di accesso*

Durante l'assenza del lavoratore il Dirigente del Settore o il responsabile del trattamento può accedere a dati e procedure del pc del lavoratore assente e verificare il contenuto dei messaggi a quest'ultimo indirizzati, a condizione che ciò si renda indispensabile e indifferibile, per esclusiva necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa

A tale scopo ogni lavoratore deve consegnare ad un altro lavoratore da lui delegato per iscritto una busta chiusa contenente le proprie password, avendo cura di sostituirla ogni volta che esse vengono cambiate.

Il lavoratore delegato, su richiesta e alla presenza del Dirigente del Settore o del responsabile del trattamento, accede ai dati e alle procedure nonché ai messaggi di posta elettronica del lavoratore assente provvedendo a inoltrare al Dirigente del Settore o al responsabile da quest'ultimo indicato quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa .

Dell'attività compiuta è redatto apposito verbale a cura del Dirigente/responsabile che ne informa il lavoratore assente alla prima occasione utile.

Nel caso in cui non sia stato delegato alcun lavoratore oppure nel caso in cui anche il lavoratore delegato non sia presente il Dirigente Responsabile di Settore/ responsabile delegato richiede ed autorizza l'intervento dei tecnici dell'Ufficio Sistema e Reti, che ne permettono l'accesso per il tempo necessario.

Questo intervento verrà documentato mediante apposito verbale redatto a cura del Dirigente Responsabile del Settore/ responsabile delegato e comunicato al lavoratore alla prima occasione utile.

Gli interventi dei tecnici dell'Ufficio Sistema e Reti possono avvenire senza conoscere e senza modificare la password del lavoratore, grazie ad una password di servizio custodita dal preposto, secondo le regole tecniche previste dalla legge.

### *Interventi di Manutenzione*

Quando per un PC occorre fare un intervento di manutenzione, ordinaria o straordinaria, sul loco o in laboratorio, sarà cura del lavoratore concordare modi e tempi di intervento con i tecnici addetti.

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

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

### ***3.4 Società esterne o professionisti per la manutenzione e l'assistenza***

Il Dirigente del Settore Sistemi Informativi e Servizi Demografici nomina la società che effettua la manutenzione dei sistemi hardware o software responsabile del trattamento dei dati utilizzando l'allegato modella A1) il quale andrà integrato con una specifica assunzione di impegno da parte del responsabile stesso al rispetto delle seguenti disposizioni:

- a) non effettuare copie né procedere alla eliminazione degli archivi informatici di titolarità dell'ente detenuti.
- b) informare preventivamente gli interessati del giorno e dell'orario in cui saranno effettuati gli interventi tecnici.
- c) richiedere preventivamente l'autorizzazione ai tecnici dell'Ufficio Sistema e Reti nel caso di interventi di assistenza tramite collegamento remoto. Gli stessi tecnici dovranno essere avvisati al termine delle operazioni.

- d) usare riservatezza su dati ed informazioni addivenuti in loro possesso.
- e) trasmettere al Dirigente del Settore Sistemi Informativi e Servizi Demografici, all'inizio della collaborazione e, successivamente, per i contratti di durata superiore all'anno, ogni dieci mesi, l'elenco aggiornato degli incaricati al trattamento
- f) nel caso che gli incaricati, per svolgere la propria attività, necessitino di accedere ad uffici e locali del Comune, informare in ogni caso tempestivamente l'Ufficio Sistema e Reti di ogni revoca e di ogni nuovo incarico conferito.

### ***3.5 Dismissione delle stazioni di lavoro***

In caso di dismissione di vecchi PC, il Dirigente che ha in carico la stazione di lavoro deve comunicare al soggetto preposto alla pulizia la presenza di banche dati da recuperare. Il soggetto preposto una volta recuperate le banche dati, conserva la stazione di lavoro per un mese quindi provvede a rendere illeggibili i dischi magnetici prima della rottamazione.

I dischi dei PC usati che il Comune cede in comodato d'uso prima della consegna vengono riformattati impedendo l'accesso alle banche dati che vi erano contenute.

### **4) Salvataggio dei dati**

Il salvataggio delle banche dati esistenti sui server è in carico all'Ufficio Sistema e Reti.

Sui sistemi centralizzati vengono fatte copie quotidiane degli archivi documentali e delle banche dati strutturate allo scopo di fornire almeno una versione aggiornata alla notte precedente.

Le copie vengono effettuate su cassette a nastro magnetico ad alta capacità contenute all'interno di due librerie automatizzate, residenti l'uno presso l'Ufficio Sistema e Reti e l'altro, di backup, presso una sede remota.

L'esecuzione dell'operazione di salvataggio è verificata quotidianamente dagli operatori di sala macchine.

Ogni singolo lavoratore è responsabile del salvataggio degli archivi esistenti sul proprio PC.

Le banche dati residenti solo sul singolo PC ( escludendo pertanto, ad esempio, le banche dati che il lavoratore ha creato per esigenze di funzionalità, quelle di cui esiste una copia cartacea ed in genere, quelle che è possibile ricostruire attingendo ad altre banche dati ) sono copiate su

supporto elettronico a disposizione del singolo lavoratore. Spetta al Dirigente di Settore effettuare periodicamente una verifica sulla presenza di banche dati residenti solo su singolo PC e richiedere all'Ufficio Sistema e Reti il supporto elettronico occorrente per il salvataggio dei dati. Tempi e modalità del salvataggio dei dati trattati, che dovrà avvenire con cadenza almeno settimanale, sono definiti nelle istruzioni impartite dai Dirigenti di Settore.

I supporti contenenti le copie di backup effettuate dai singoli utenti, quando non più utilizzati, possono essere archiviati o distrutti, ma non utilizzati per altre tipologie di dati o per la trasmissione all'esterno.

## **5) Locali**

I locali dove risiedono fisicamente i server e la prima libreria robotizzata sono dotati di alcuni accorgimenti minimi a garanzia sia della sicurezza fisica dell'hardware, sia delle banche dati:

1. chiusura di sicurezza per la porta di ingresso ai locali, ed accesso controllato da videocitofono per i dipendenti autorizzati;
2. stabilizzatore di temperatura per i locali;
3. gruppo di continuità e di stabilizzazione della corrente;
4. cassaforte ignifuga per cassette, dischetti e CD di salvataggio;
5. impianto di rilevamento fumi e spegnimento automatico in caso di incendio, collegato con la sede di una società di sicurezza e pronto intervento;
6. impianto antintrusione collegato con la sede di una società di sicurezza e pronto intervento

Il locale dove risiede la seconda libreria automatizzata è dotato di:

7. chiusura di sicurezza per la porta di ingresso al locale;
8. stabilizzatore di temperatura per i locali;
9. gruppo di continuità e di stabilizzazione della corrente.

## **6) Cautele generali**

### ***6.1 Password***

La password deve essere composta da almeno 8 caratteri.

Le Password non devono contenere riferimenti agevolmente riconducibili all'incaricato e devono essere modificate almeno **ogni tre mesi**.

I sistemi centralizzati di autenticazione provvedono in modo automatico alla scadenza trimestrale della password.

E' responsabilità dell'utente provvedere alla modifica della password del PC almeno ogni tre mesi.

## ***6.2 Uso del Computer***

Il Dirigente di Settore/ responsabile delegato deve impartire le istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro.

Se il PC viene lasciato acceso incustodito, l'utente attivo al momento deve essere disconnesso o deve essere attivata la modalità salvaschermo con protezione mediante password.

## ***6.3. Custodia dei supporti***

Devono essere impartite, da parte del Responsabile del trattamento, 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

## **7 ) QUADRO RIEPILOGATIVO DELLE BANCHE DATI E DEI RELATIVI CODICI**

*Codici di riferimento per la classificazione delle banche dati :*

Codice	Descrizione	Misure di Sicurezza	
		Tipologia	Responsabilità
1	Banca dati informatizzata , centralizzata	tecnica e organizzativa	Progetti Telematici Sistemi e Reti
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	Progetti Telematici Sistemi e Reti
4	Banca dati residente su supporti di memorizzazione non in linea (CD ROM, DVD, Dischetti, Nastro magnetico)	tecnica e organizzativa	incaricato

Le Determinazioni di specificazione del presente documento dovranno fare riferimento , nelle schede descrittive ( allegato “B” ), ai codici sopra evidenziati. Qualora per un particolare trattamento i codici siano più di uno, vanno indicati tutti.

## **B) Documento programmatico sulla sicurezza**

Il presente documento, considerate le caratteristiche organizzative dell’Ente, rinvia alcuni adempimenti alle determinazioni che i singoli Dirigenti di Settore, in quanto titolari del trattamento dei dati, devono adottare e precisamente:

1. l’elenco dei trattamenti di dati personali;
2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati ovvero la nomina dei Responsabili dei trattamenti e degli Incaricati .
3. l’analisi dei rischi che incombono sui dati.
- 4 .Le misure ulteriori da adottare, aggiuntive rispetto a quelle indicate nei seguenti punti 4.1, 4.2, 4.3, 4.4 per garantire l’integrità e la disponibilità dei dati

### *Altri adempimenti:*

4.1 Le misure da adottare per garantire l'integrità e la disponibilità dei dati elettronici, sono state dettagliatamente evidenziate al punto A del presente Disciplinare Tecnico.

4.2 Il Servizio Prevenzione e Protezione, del Settore Lavori Pubblici, dovrà garantire la protezione delle aree e dei locali, con specifico riferimento ai Piani di Emergenza elaborati per le diverse Strutture Comunali.

4.3 Il Servizio Finanze ed Economato dovrà provvedere alle autorizzazioni ad accedere ai locali al di fuori dell'orario di lavoro del personale dell'impresa di pulizia per le sedi oggetto di appalto.

4.4 l'accesso al Palazzo Comunale dopo l'orario di chiusura è garantito dal personale di sorveglianza gestito dal Servizio Finanze ed Economato ed anche a mezzo di strumenti di Videosorveglianza degli accessi installati dal Settore Manutenzione e Logistica. L'accesso dopo l'orario di chiusura nei palazzi, sede di uffici comunali: Via Galaverna 8, Via Santi 40, Via Santi 60 , è consentito ad amministratori e lavoratori autorizzati in quanto titolari di apposito badge identificativo personale che attiva il dispositivo per l'apertura degli ingressi; l'accesso agli uffici comunali di Via Costa 13 è consentito ad amministratori e lavoratori autorizzati solo attraverso apposito badge identificativo personale. Il Settore Manutenzione e Logistica cura la gestione dei sistemi di allarme esistenti nei palazzi di Via Galaverna 8, Via Santi 40, Via Santi 60 , Via Costa 13 .

5. Il Servizio Progetti Telematici e l'Ufficio Sistema e Reti in conformità alle disposizioni di legge provvedono alla descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento.

6. Il Settore Personale, Organizzazione e Semplificazione Amministrativa, Privacy - Qualità dovrà curare la formazione dei dipendenti in special modo nei confronti dei nuovi assunti. In modo particolare il programma di formazione dovrà :

- a) rendere consapevoli i partecipanti sull'importanza delle scelte dell'Ente;
- b) coinvolgere i partecipanti sulle problematiche inerenti alla sicurezza;
- c) responsabilizzare i partecipanti sulle attività da eseguire.

I corsi saranno progettati in base alle diverse esigenze ed ai diversi sistemi di sicurezza sviluppati, in funzione al grado di informatizzazione raggiunto; in generale non potranno mancare riferimenti a:

- normativa vigente;
  - definizione delle responsabilità;
  - elenco delle vulnerabilità: spesso non c'è la consapevolezza dei rischi che si possono correre.
- regole comportamentali che comprendono la gestione degli accessi (password.);
- regole comportamentali di riservatezza sia in orario di lavoro sia al di

- fuori dell'ambito lavorativo;
- i possibili rischi: virus, intercettazioni, intrusioni, ecc..

7. Ogni Settore provvede:

- alla conservazione separata dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali trattati per finalità che non richiedono il loro utilizzo;
- all'adozione di codici identificativi o soluzioni analoghe che rendano i dati sensibili e giudiziari contenuti in elenchi, registri, banche dati tenuti con l'ausilio di strumenti elettronici temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. Per tale attività i Settori si avvalgono , qualora lo ritengano opportuno, dell'ausilio del Settore Sistemi Informativi

8. Il Comune è impegnato in un processo di valorizzazione dell'utilizzo della rete telematica, ma è consapevole che tale impegno deve essere attuato nel pieno rispetto delle previsioni normative, dei principi di necessità, pertinenza e non eccedenza dei dati personali, del diritto all'oblio e dei diritti fondamentali della persona.

In particolare, sono allo studio ed in via di sperimentazione forme adeguate di selezione dei dati pubblicati sul sito web del Comune che evitino, per quanto possibile, che i comuni motori di ricerca esterni possano, in qualsiasi momento, in modo massivo e indiscriminato, reperire un insieme di dati personali resi disponibili in rete.

Sarà pertanto cura di ogni singolo Dirigente di Settore individuare, volta per volta, i casi in cui è necessario o opportuno che documenti, atti, informazioni del proprio Settore, pur rimanendo accessibili attraverso la pubblicazione sul sito web del Comune, vengano trattati con le tecniche più adeguate per escludere selettivamente l'accesso dei motori di ricerca. A tal fine, il Dirigente di Settore, nei casi sopra indicati, dovrà concordare con il Servizio Comunicazione, Marketing e Rapporti con i cittadini del Settore Direzione Generale l'adozione delle misure più opportune allo scopo ( attraverso, ad esempio , l'inserimento nella pagina web di opportuni comandi o l'attribuzione alle sole persone interessate di una chiave personale di accesso )

In ogni caso, sarà cura del Dirigente di Settore individuare il periodo temporale entro il quale si potrà ritenere proporzionato, in rapporto alle finalità perseguite, mantenere sul sito del Comune documenti, atti, informazioni sia che essi siano direttamente individuabili anche tramite

motori di ricerca esterna sia che l'azione dei motori di ricerca sia limitata o inibita.

9. Il Dirigente del Settore Sistemi Informativi e Servizi Demografici ha provveduto con propria determinazione a redigere l'elenco degli amministratori di sistema del Comune e a designarli individualmente con successivo atto precisandone le funzioni e specificandone l'ambito di attività.

Gli estremi identificativi delle persone fisiche designate, con l'indicazione delle funzioni ad esse attribuite, è riportato in un elenco agli atti del settore stesso. Con cadenza annuale il Dirigente del Settore Sistemi Informativi e Servizi Demografici verifica l'operato degli amministratori di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle normative vigenti.

Il Settore Sistemi Informativi e Servizi Demografici ha adottato le misure necessarie a consentire un'attività di verifica dell'operato degli amministratori di sistema alla luce delle normative vigenti in merito al trattamento dei dati personali.

### **C) Il Trattamento dei dati senza l'ausilio di strumenti elettronici**

Il trattamento "cartaceo" di dati personali deve essere garantito da particolari misure minime di sicurezza che debbono essere specificate dal Titolare del Trattamento dei dati nelle istruzioni impartite ai responsabili ed agli incaricati per le diverse tipologie di trattamento, in particolare:

*Il responsabile 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 Settore Sistemi Informativi
- formulare proposte per l'eventuale distruzione, se consentito dalle norme, dei documenti contenenti dati non più necessari.

*L'incaricato 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, fare pronta denuncia al responsabile;
- in caso di assenza dall'ufficio per cui il medesimo risulti non presidiato, proteggere in luogo custodito i singoli documenti temporaneamente estratti dall'archivio per motivi di lavoro e non lasciarli sulle scrivanie o alla libera visione di terzi;
- evitare di effettuare il trattamento dei dati personali in presenza di

terzi che possano così venire a conoscenza, anche occasionalmente, dei dati.

**1 ) QUADRO RIEPILOGATIVO DELLE MISURE MINIME PER I TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI E DEI RELATIVI CODICI**

Codici di riferimento per la classificazione

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 Peg/ responsabile
8	Rilascio autorizzazione formale agli incaricati con le istruzioni per tutti gli operatori	organizzativa	Dirigente Peg/ responsabile

Le Determinazioni di specificazione del presente documento dovranno fare riferimento nelle schede descrittive ( allegato B ), ai codici impiegati per la protezione dei dati, sopra evidenziati. Qualora per un particolare trattamento i codici siano più di uno, vanno indicati tutti.

## **ALLEGATI:**

- “A1” - Designazione responsabile esterno del trattamento
- “A2 “- Nomina incaricato al trattamento dei dati ( soggetti esterni )
- “B” Fac- simile scheda rilevazione Trattamento Dati Personali , Sensibili e giudiziari da allegare alla determinazione dirigenziale
- “ C “ Convenzione per l'accesso in consultazione alla banca dati informatizzata dell'anagrafe del Comune di Modena e per l'eventuale trasmissione in fruizione dei dati anagrafici

*Comune di Modena  
Settore .....*

*A .....*  
*.....*

*Oggetto: Designazione responsabile del trattamento di dati personali*

**IL DIRIGENTE**

*Richiamati:*

- *la disposizione del Sindaco del ..... prot. n. .... , con la quale il sottoscritto è stato nominato titolare delle banche dati e del trattamento dei dati personali del settore .....*;
- *l'art.29 del dlgs n.196/2003 "Codice in materia di protezione dei dati personali", relativo al Responsabile del trattamento;*
- *l'art.16 del Regolamento per l'accesso agli atti, ai documenti ed alle informazioni e per la tutela dei dati personali, approvato con deliberazione del Consiglio Comunale n.157 del 4/7/1994, modificato ed integrato con deliberazioni del Consiglio Comunale nn. 4 e 97 del 1999 e n.68 del 30.10.2006 ;*
- *il Disciplinare Tecnico in materia di misure minime di sicurezza approvato con la deliberazione della Giunta Comunale n.....del .....*;
- *il Regolamento per la protezione dei dati personali per effettuare il trattamento dei dati sensibili e giudiziari " approvato con deliberazione*
- *della Giunta Comunale n.763 del 29/11/2005 successivamente integrata con deliberazioni della Giunta Comunale nn. 224 e 495 del*

2006 e n.80 del 27/2/2007;

- *il contratto/ convenzione / concessione stipulato in data .....;*
- *Considerato che sussistono i requisiti di esperienza, capacità e affidabilità di cui all'art. 29, comma 2, del decreto legislativo 30 giugno 2003 n. 196;*

Visto il D.lgs. 267/2000;

*Designa*

\_\_\_\_\_ con sede in \_\_\_\_\_ nella persona  
di-----

*Responsabile del trattamento dei dati personali effettuato nello svolgimento di operazioni strettamente necessarie e strumentali rispetto all'esecuzione del contratto/ convenzione/concessione.*

*In tale qualità, \_\_\_\_\_ è tenuto al rispetto delle disposizioni di legge e di regolamento in materia di tutela dei dati personali.*

*In particolare:*

- *osservare il decreto legislativo 30 giugno 2003 n. 196 e le altre disposizioni legislative e regolamentari in materia di riservatezza delle persone osservando i principi di liceità e correttezza;*
- *censire i trattamenti di dati personali e le banche dati gestite per conto dell'amministrazione;*
- *nominare gli incaricati del trattamento sulla base dello schema di incarico fornito dal Comune nonché impartire loro le istruzioni necessarie per un corretto, lecito, sicuro trattamento dei dati e per la loro custodia;*
- *tenere un elenco aggiornato degli incaricati del trattamento che dovrà essere fornito, a richiesta, al Comune ;*
- *coordinare tutte le operazioni di trattamento dei dati e vigilare sull'osservanza delle istruzioni impartite;*
- *attuare gli obblighi di informativa nei confronti degli interessati;*
- *garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del decreto legislativo 30 giugno 2003 n. 196, riferendo in ogni caso all'ufficio \_\_\_\_\_;*

- *collaborare per l'attuazione delle prescrizioni del Garante;*
- *predisporre e aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni agli articoli da 31 a 36 e allegato B del decreto legislativo 30 giugno 2003 n. 196 e da ogni altra disposizione in materia, nonché adeguare il sistema alle future norme regolamentari in materia di sicurezza;*
- *elaborare una relazione trimestrale sullo stato degli adempimenti previsti dal decreto legislativo 30 giugno 2003 n. 196.*

*Nel caso in cui l'oggetto del contratto o della convenzione comporti l'utilizzazione di applicazioni o banche dati del Comune, per ottenere le relative autorizzazioni all'accesso il responsabile esterno dovrà fornire al Dirigente del Settore all'inizio della collaborazione, l'elenco degli incaricati al trattamento dei dati per i quali si richiede il rilascio delle credenziali. Le credenziali che abilitano gli incaricati alle applicazioni e alle banche dati hanno una durata massima di dodici mesi, trascorsi i quali esse verranno automaticamente disabilitate. Pertanto, qualora il contratto/ convenzione/ concessione abbia una durata superiore all'anno, il responsabile esterno del trattamento dei dati, al fine di evitare che le credenziali degli incaricati siano automaticamente disabilitate alla scadenza dei dodici mesi, dovrà fornire all'amministrazione, due mesi prima della scadenza delle stesse, l'elenco aggiornato degli incaricati che sostituirà quello precedentemente fornito.*

*Qualsiasi utilizzo e trattamento del dato improprio o non conforme al Dlgs. 196/2003 comporterà l'esclusiva e piena responsabilità della società / ente ....., rimanendo il Comune escluso da ogni responsabilità al riguardo*

*Data*

*Il Dirigente*

*Per accettazione ( data, qualifica e firma ) .....*

Sig.

*Oggetto: Nomina incaricato del trattamento di dati personali*

*La società / ente ..... nella persona  
di .....*

*premesso che, con atto PG ..... del ....., è stata designata responsabile del  
trattamento dei dati personali effettuato nello svolgimento di operazioni  
strettamente necessarie e strumentali rispetto all'esecuzione del contratto/  
convenzione/concessione stipulato con il Comune di Modena in  
data .....*

*richiamato l'art. 30 del dlgs n.196/2003 "Codice in materia di protezione dei  
dati personali", relativo agli Incaricati del trattamento;*

*incarica*

*il Sig.....delle seguenti operazioni di trattamento :*

.....  
.....

*A tal fine impartisce le seguenti istruzioni:*

- I dati possono essere trattati esclusivamente per gli scopi definiti  
dall'ambito di trattamento indicato e non possono in alcun modo essere  
comunicati a terzi non incaricati.*

*-Una volta portato a termine l'incarico assegnato, non si potrà conservare  
copia dei dati e dei programmi del Comune di Modena né alcuna  
documentazione ad essi inerente:*

- *Devono essere osservate 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.*
- *A tale fine deve essere assicurata la custodia e la riservatezza dei dispositivi di autenticazione per il trattamento con l'ausilio di strumenti elettronici, e non deve essere lasciato incustodito e accessibile lo strumento elettronico durante una seduta di trattamento, anche in caso di assenza temporanea dall'ufficio (es. pausa caffè) in particolare negli orari di accesso agli uffici da parte del pubblico esterno.*
- *Analogamente deve essere assicurata la custodia delle chiavi di locali, armadi e cassettiere in cui sono conservati i documenti contenenti dati personali e, in caso di furto o smarrimento, deve essere fatta pronta denuncia al responsabile.*
- *In caso di assenza dall'ufficio per cui il medesimo risulti 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.*

*Il Responsabile*

*Per ricevuta .....*  
*Modena, .....*

## *ALLEGATO B)*

	Tipologia di trattamento	Tipologia dati (1)	Tipologia di Banca Dati /Archivi	Nome del Responsabile	Servizio / Ufficio (4)	Codici (2) (3)	Ubicazione fisica	Comunicazioni e dei dati
1								
2								
3								

1) Specificare tipo di dati: personali, sensibili, giudiziari.

2) Indicare, come da quadro riepilogativo, i codici delle banche informatizzate.

3) Indicare i codici delle misure di sicurezza per trattamenti senza ausilio di strumenti elettronici, come da relativa tabella. Specificare eventuali casi particolari.

4) Indicare il nome del Servizio/Ufficio riportato nella determinazione dirigenziale con cui è stata approvata, all'inizio dell'anno, l'articolazione della struttura organizzativa interna del Settore e l'assegnazione del personale agli uffici.

**CONVENZIONE TRA IL COMUNE DI MODENA E ..... PER  
L'ACCESSO IN CONSULTAZIONE ALLA BANCA DATI INFORMATIZZATA  
DELL'ANAGRAFE DEL COMUNE DI MODENA E PER L'EVENTUALE  
TRASMISSIONE IN FRUIZIONE DEI DATI ANAGRAFICI**

Il Comune di Modena, in seguito denominato Comune, con sede in .....  
cod. fiscale ..... rappresentato da ..... nella qualità di  
dirigente del Settore Sistemi Informativi e Servizi Demografici e titolare del  
trattamento della banca dati anagrafica

e

....., in seguito denominato Ente , con sede  
in ..... cod. fiscale ..... rappresentato da ..... nella  
propria qualità di .....

- vista la nota del ..... pervenuta al protocollo generale in data  
..... n..... con la quale ..... ha chiesto l'autorizzazione  
alla consultazione telematica dell'archivio anagrafico e alla trasmissione  
in fruizione dei dati anagrafici essenziali per lo svolgimento dei propri  
compiti istituzionali, specificando gli adempimenti normativi e le finalità  
istituzionali perseguite;
- valutata la legittimità della richiesta in considerazione delle motivazioni di  
pubblica utilità rappresentate;
- vista la propria determinazione n. .... del ..... con la quale si  
ritiene di addivenire alla stipula della convenzione;
- richiamata la delibera della Giunta Comunale n..... del .....  
con cui è stato definito lo schema di convenzione per la consultazione e  
l'accesso ai dati anagrafici

Visti:

- la Legge 24/12/1954 n.1228 (Legge anagrafica);
- il D.P.R. 30/5/1989 n.223 (Regolamento anagrafico);
- l'art. 2 della Legge 17/3/1993 n.63 e il DPCM 5/5/1994 in tema di  
collegamenti telematici;
- l'art. 2, comma 5 della Legge 15/5/1997 n.127;
- l'art. 43 del D.P.R.28/12/2000 n.445;
- il Dlgs 30/3/2003 n.196 (Codice della privacy);
- il Dlgs 7/3/2005 n.82 (Codice dell'Amministrazione Digitale)

convengono quanto segue

### **Art.1 – Definizioni**

**Ente** : la pubblica amministrazione, il concessionario e il gestore di un pubblico servizio che abbia necessità di accedere alle informazioni anagrafiche per finalità istituzionali

**Consultazione dei dati**: la possibilità di accedere al dato in sola visualizzazione e lettura senza che sussista un sistema tecnologico che ne consenta l'estrazione. Il dato rimane, pertanto, all'interno del sistema informativo proprietario

**Fruizione dei dati**: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione o ente. Il trasferimento del dato non ne modifica la titolarità.

**Visura anagrafica**: documento informatico erogato, ai sensi dell'articolo 43, comma 4 del DPR 445/2000, dal sistema informativo del Comune di Modena, avente la forza probatoria di cui all'art. 2712 c.c. " riproduzione informatica " e contenente informazioni anagrafiche certificate per le pubbliche amministrazioni, concessionari e gestori di pubblici servizi.

### **Art. 2 Oggetto della convenzione**

Il Comune autorizza l'accesso alla banca dati informatizzata degli archivi anagrafici e alla trasmissione dei dati anagrafici per le specifiche finalità istituzionali secondo le modalità e nei limiti specificati nei successivi articoli.

A tal fine l'Ente si impegna a:

- Utilizzare l'accesso alla banca dati per la consultazione delle sole informazioni la cui conoscenza è necessaria, pertinente e non eccedente ai fini dello svolgimento delle operazioni di trattamento indicate nella richiesta e finalizzate al perseguimento delle finalità istituzionali
- Svolgere il servizio di consultazione nel rispetto della normativa vigente in materia e secondo le modalità di seguito specificate.

L'accesso alle informazioni anagrafiche avverrà sulla base di visure anagrafiche dettagliate nell'allegato 1 .

L'Ente si impegna a non richiedere al Comune controlli sulle autocertificazioni rese dai cittadini o comunque informazioni su dati che possono essere assunti attraverso l'accesso alla banca dati anagrafica.

L'accesso a dati ulteriori rispetto a quelli contenuti nelle visure di cui all'allegato 1 potranno essere autorizzate solo se l'Ente motiverà la propria richiesta sulla base di specifiche finalità e competenze istituzionali dichiarando, nel contempo la pertinenza e necessità dei dati richiesti.

### **Art. 3 – Dato oggetto della consultazione/fruizione**

Il Comune consente l'accesso telematico tramite la rete Internet ad un servizio di consultazione anagrafica che rende disponibili le informazioni sotto forma di visure secondo il dettaglio riportato nell'allegato 1, che costituisce parte integrante della presente convenzione.

L'accesso a tali dati è consentito nel rispetto del principio di necessità, pertinenza e non eccedenza dei dati e del trattamento rispetto alle finalità e competenze istituzionali perseguite dall'Ente.

L'Ente si impegna a comunicare tempestivamente ogni innovazione normativa/organizzativa che comporti una revisione della presente convenzione. In tal caso il Comune si riserva di modificare la convenzione e le modalità di accesso ai dati sulla base delle innovazioni normativa e/o organizzative intervenute.

Qualora l'Ente abbia la necessità di disporre, ai fini della fruizione, di elenchi di dati dovrà trasmettere all'Ufficio Anagrafe lo schema dei dati anagrafici da estrarre, la loro logica, formato e codifiche, indicando le motivazioni e le disposizioni normative o regolamentari che ne legittimano la fruizione.

Non è consentito duplicare, riprodurre, cedere e/o diffondere i dati contenuti nella banca dati, comunicarli a soggetti non autorizzati o utilizzarli per fini diversi da quelli contemplati nella presente convenzione.

### **Art. 4 – Titolarità della banca dati**

Il Comune conserva la piena ed esclusiva proprietà delle informazioni contenute nella banca dati anagrafica e del sistema di ricerca; ha l'esclusiva competenza di gestire, definire e modificare i sistemi di elaborazione, ricerca, rappresentazione e organizzazione dei dati; ha altresì la facoltà di variare la base informativa in relazione alle proprie esigenze istituzionali, organizzative e tecnologiche.

La banca dati anagrafica è di esclusiva titolarità del Comune.

Qualora intervengano modificazione delle circostanze di fatto e di diritto, l'Ente ha la facoltà di recedere dalla presente convenzione, previo preavviso di almeno trenta giorni da inviare al Comune con raccomandata con ricevuta di ritorno o strumento equivalente (posta elettronica certificata).

### **Art. 5 – Responsabile del trattamento**

L'Ente si impegna ad individuare, designare e comunicare tempestivamente al Comune il nominativo del responsabile del trattamento dei dati alla cui nomina si provvederà, ai sensi dell'articolo 29 del Dlgs 196/2003, con specifico atto di cui all'allegato 2, nel rispetto delle prescrizioni e delle modalità di cui al Disciplinare Tecnico in materia di misure di sicurezza adottato dal Comune di Modena, che l'Ente dichiara di ben conoscere e che si impegna a rispettare.

In caso di sostituzione del responsabile, l'Ente si impegna a comunicare

tempestivamente il nominativo del nuovo responsabile al Comune che provvederà alla nomina dello stesso.

### **Art. 6 - Abilitazione all'interrogazione della banca dati**

L'Ente si impegna a comunicare al Comune l'elenco degli utenti che devono essere abilitati all'interrogazione della banca dati, allegando una scheda identificativa nella quale devono essere indicate le seguenti informazioni:

- nome e cognome
- codice fiscale
- numero di telefono e sede di lavoro

L'Ente si impegna ad incaricare del trattamento ogni operatore indicato in elenco utilizzando l'allegato 3 e a responsabilizzarlo in ordine al corretto utilizzo dei dati, alle problematiche inerenti alla sicurezza e a quanto stabilito dalla presente convenzione.

### **Art. 7 – Modalità di accesso**

Alla banca dati anagrafica potranno accedere esclusivamente gli incaricati di cui all'articolo 6 dotati delle proprie credenziali d'accesso.

Al fine di consentire lo svolgimento dell'attività di consultazione della banca dati, il Comune si impegna a fornire in busta chiusa ad ognuno dei suddetti operatori le credenziali di autenticazione individuali (userid e password provvisoria).

Al primo accesso al sistema informatico, gli incaricati del trattamento dei dati dovranno sostituire la password provvisoria loro assegnata con una di loro scelta.

L'Ente si impegna a far sì che i propri utenti mantengano la password segreta, che venga conservata adeguatamente e che non venga né comunicata né divulgata. La password dovrà essere modificata alle scadenze temporali indicate nel Disciplinare Tecnico delle misure minime di sicurezza del Comune di Modena.

In caso di cessazione di un operatore dall'incarico, l'Ente si impegna a darne tempestiva notizia al Comune tramite l'indirizzo e.mail ..... affinché venga disabilitato.

Non è consentito l'accesso contemporaneo da più postazioni di lavoro con il medesimo identificativo.

Il collegamento è consentito agli operatori incaricati esclusivamente durante lo svolgimento della propria attività lavorativa.

Le stazioni di lavoro collegate con la banca dati comunale dovranno essere collocate in luogo non accessibile al pubblico e poste sotto la responsabilità dell'operatore designato.

L'Ente si impegna inoltre a compiere, attraverso il responsabile del trattamento, periodici controlli sugli accessi effettuati da parte degli operatori, informando immediatamente il Comune di eventuali anomalie riscontrate.

## **Art. 8 – Comunicazioni obbligatorie a carico del responsabile del trattamento**

Le credenziali di autenticazione hanno una durata massima di 12 mesi. Al fine di evitare che le credenziali degli operatori incaricati siano automaticamente disabilitate allo scadere dei 12 mesi, il responsabile del trattamento dei dati è tenuto, due mesi prima della scadenza delle stesse, a comunicare per iscritto al Comune l'elenco aggiornato degli incaricati in sostituzione di quello precedentemente fornito, dando altresì conferma del permanere delle finalità e delle motivazioni per cui è stato concesso l'accesso alla banca dati anagrafica.

## **Art. 9 - Misure di sicurezza**

La consultazione dei dati avverrà mediante accesso telematico tramite la rete Internet, nelle modalità concordate con il Comune .

L'Ente garantisce l'adeguatezza del proprio standard di sicurezza della protezione dei dati e l'adozione di ogni misura necessaria ad evitare indebiti utilizzi dei dati stessi, dichiarandosi fin d'ora disponibile a seguire anche le indicazioni tecniche fornite dal Comune.

L'Ente si impegna a fornire, a richiesta del Comune, le specifiche tecniche dei sistemi di sicurezza dei propri collegamenti informatici con la banca dati comunale.

Il Comune è legittimato a registrare tutti gli accessi sul proprio sistema informativo memorizzando le posizioni interrogate in appositi files, al fine di prevenire o correggere malfunzionamenti del sistema e garantire l'efficienza dello stesso e di mettere i file a disposizione dell'autorità giudiziaria, qualora richiesti. Tali registrazioni verranno conservate per un periodo di tempo di -----

I sistemi di sicurezza sopra descritti saranno disabilitati per le Forze di Polizia, Carabinieri, Guardia di Finanza, Corpo Forestale dello Stato, Polizia Municipale, Procura, Tribunali al fine di salvaguardare il preminente interesse alla riservatezza delle indagini.

## **Art. 10– Limitazione e responsabilità**

Il Comune è sollevato da ogni responsabilità contrattuale ed extracontrattuale per danni diretti o indiretti che possano derivare in conseguenza dell'uso dei dati attinti dalla banca dati anagrafica/stato civile del Comune nonché per i danni derivanti da interruzioni, ritardi o errori nella elaborazione e/o trasmissione dei dati, ovunque si verificano, in qualunque forma si manifestino e da qualsiasi causa siano determinati.

L'Ente si impegna ad utilizzare le informazioni ottenute tramite il collegamento esclusivamente per fini istituzionali, nel rispetto della normativa vigente, dei principi di necessità, pertinenza e non eccedenza e del diritto alla riservatezza e si assume ogni responsabilità in ordine all'utilizzo e al trattamento improprio

o illecito e alle conseguenti eventuali richieste di risarcimento da parte di terzi, sollevando al riguardo il Comune da ogni responsabilità.

#### **Art.11 - Costi**

La consultazione della banca dati è fornita gratuitamente dal Comune. Sono a carico dell'Ente i costi relativi all'attivazione del collegamento.

#### **Art.12 - Durata**

La presente convenzione avrà durata di 4 anni dalla data di sottoscrizione con possibilità di rinnovo esplicito per altri 4 anni.

Il Comune si riserva la possibilità di recedere in qualsiasi momento dalla presente convenzione a suo insindacabile giudizio, previa comunicazione inviata con raccomandata con ricevuta di ritorno o altro strumento analogo, qualora non siano rispettate le condizioni in essa previste o nel caso del verificarsi di eventi che motivino la cessazione della comunicazione dei dati (interventi normativi, ecc.).

#### **Art.13 – Foro competente**

Per tutte le controversie direttamente o indirettamente connesse alla presente convenzione è competente il Foro di Modena.

#### **Art.14 - Registrazione**

La presente convenzione, redatta in due originali, non è soggetta a registrazione ai sensi dell'art.1 della tabella allegata al DPR 26.4.1986 n.131

#### **Art.15 – Spese contrattuali**

Non sono previste spese contrattuali.

#### **Art. 16 Informativa**

Le parti dichiarano di essersi scambiati la reciproca informativa ai sensi dell'art.13 del Dlgs 196/2003

Modena, .....

**(elenco possibili visure. Da modulare sulla base della profilazione autorizzata)**

**Visure Anagrafiche**

- Visura di residenza
- Visura di residenza – AIRE
- Visura di cittadinanza
- Visura di carta d'identità
- Visura di codice fiscale
- Visura di famiglia
- Visura di famiglia con rapporto di parentela
- Visura di dati patente e targhe inoltrati alla MCTC
- Visura di nascita
- Visura di permesso di soggiorno
- Visura di stato civile (celibe/nubile, matrimonio, divorzio, vedovanza)

La Visura Anagrafica è riprodotta ai sensi dell'art. 43, comma 4 del D.P.R. 28/12/2000 n. 445 ed ha valore di riproduzione informatica ai sensi dell'art. 2712 c.c.

**Nomina del responsabile esterno del trattamento**

A .....  
.....

Oggetto: nomina responsabile del trattamento di dati personali

IL DIRIGENTE

Richiamati:

- la disposizione del Sindaco del ..... prot. n. .... , con la quale il sottoscritto è stato nominato titolare delle banche dati e del trattamento dei dati personali del settore .....
- l'art.29 del dlgs n.196/2003 "Codice in materia di protezione dei dati personali", relativo al Responsabile del trattamento;
- l'art.16 del Regolamento per l'accesso agli atti, ai documenti ed alle informazioni e per la tutela dei dati personali, approvato con deliberazione del Consiglio Comunale n.157 del 4/7/1994, modificato ed integrato con deliberazioni del Consiglio Comunale nn. 4 e 97 del 1999 e n.68 del 30.10.2006;
- il Disciplinare Tecnico in materia di misure minime di sicurezza approvato con la deliberazione della Giunta Comunale n.....del .....
- il Regolamento relativo al trattamento dei dati sensibili e giudiziari, approvato con deliberazione della Giunta Comunale n. 763 del 29/11/2005 successivamente integrata con deliberazioni della Giunta Comunale nn. 224 e 495 del 2006 e n.80 del 27/2/2007;
- la convenzione stipulata in data .....
- la comunicazione effettuata da .....in data ..... recante da designazione di .... ....., quale soggetto idoneo a ricoprire il ruolo di responsabile del trattamento;
- Considerato che in capo al soggetto individuato e designato sussistono i requisiti di esperienza, capacità e affidabilità di cui all'art. 29, comma 2, del decreto legislativo 30 giugno 2003 n. 196;

Visto il D.lgs. 267/2000;

## NOMINA

\_\_\_\_\_ con sede in \_\_\_\_\_ nella persona di----- Responsabile del trattamento dei dati personali effettuato nello svolgimento di operazioni strettamente necessarie e strumentali rispetto all'esecuzione del contratto/convenzione/concessione.

In tale qualità, \_\_\_\_\_ è tenuto al rispetto delle disposizioni di legge e di regolamento in materia di tutela dei dati personali.

In particolare:

- osservare il decreto legislativo 30 giugno 2003 n. 196 e le altre disposizioni legislative e regolamentari in materia di riservatezza delle persone e tutela dei dati personali, osservando i principi di liceità e correttezza;
- nominare gli incaricati del trattamento sulla base dello schema di incarico fornito dal Comune nonché impartire loro le istruzioni necessarie per un corretto, lecito, sicuro trattamento dei dati e per la loro custodia;
- tenere un elenco aggiornato degli incaricati del trattamento che dovrà essere fornito, a richiesta, al Comune;
- coordinare tutte le operazioni di trattamento dei dati e vigilare sull'osservanza delle istruzioni impartite;
- attuare gli obblighi di informativa nei confronti degli interessati;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del decreto legislativo 30 giugno 2003 n. 196, riferendo in ogni caso all'ufficio \_\_\_\_\_;
- collaborare per l'attuazione delle prescrizioni del Garante;
- predisporre e aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni previste dagli articoli da 31 a 36, dall'allegato 2 del decreto legislativo 30 giugno 2003 n. 196 e da ogni altra disposizione in materia, procedendo ai successivi adeguamenti del sistema richiesti da sopravvenute norme regolamentari in materia di sicurezza;
- elaborare una relazione trimestrale sullo stato degli adempimenti previsti dal decreto legislativo 30 giugno 2003 n. 196, da comunicare su richiesta al Comune.

Nel caso in cui l'oggetto del contratto o della convenzione comporti l'utilizzazione di applicazioni o banche dati del Comune, per ottenere le relative autorizzazioni all'accesso il responsabile esterno dovrà fornire al Dirigente del Settore all'inizio della collaborazione, l'elenco degli incaricati al trattamento dei dati per i quali si richiede il rilascio delle credenziali. Le credenziali che abilitano gli incaricati all'utilizzazione delle applicazioni e delle banche dati hanno una durata massima di dodici mesi, trascorsi i quali esse verranno automaticamente disabilitate. Pertanto, qualora il contratto/convenzione/concessione abbia una durata superiore all'anno, il responsabile esterno del trattamento dei dati, al fine di evitare che le credenziali degli incaricati siano automaticamente disabilitate alla scadenza dei dodici mesi, dovrà fornire all'amministrazione, due mesi prima della scadenza delle stesse, l'elenco aggiornato degli incaricati che sostituirà quello precedentemente fornito. Qualsiasi utilizzo e trattamento del dato improprio o non conforme al Dlgs. 196/2003 comporterà l'esclusiva e piena responsabilità della società/ente ....., rimanendo il Comune escluso da ogni responsabilità al riguardo.

Il Dirigente  
-----

Data .....

Per accettazione ( data, qualifica e firma ) .....

**Nomina dell'incaricato esterno del trattamento**

Sig. ....

Oggetto: Nomina dell'incaricato del trattamento di dati personali

L'ente..... nella persona di .....

premesso che, con atto PG ..... del ....., è stato designato responsabile del trattamento dei dati personali per lo svolgimento delle operazioni strettamente necessarie e strumentali rispetto all'esecuzione della convenzione stipulata con il Comune di Modena in data .....

richiamato l'art. 30 del dlgs n.196/2003 "Codice in materia di protezione dei dati personali", relativo agli Incaricati del trattamento;

incarica

il Sig.....delle seguenti operazioni di trattamento :

.....  
.....

A tal fine impartisce le seguenti istruzioni

- I dati possono essere trattati esclusivamente per gli scopi definiti dall'ambito del trattamento indicato e non possono in alcun modo essere comunicati a terzi non incaricati.
- Concluso l'incarico assegnato, non potrà conservare copia dei dati e dei programmi del Comune di Modena né alcuna documentazione ad essi inerente.
- Devono essere osservate le norme di diligenza, prudenza e cautela finalizzate a prevenire ed evitare lo smarrimento, la distruzione o la perdita di documenti contenenti dati personali, nonché l'accesso o il trattamento da parte di persone non autorizzate.
- A tale fine deve essere assicurata la custodia e l'uso esclusivo e personale dei dispositivi di autenticazione rilasciati per il trattamento con l'ausilio di strumenti elettronici, e non deve essere lasciato incustodito e accessibile lo strumento elettronico durante la sessione di trattamento, anche in caso di assenza temporanea dall'ufficio (es. pausa caffè) e in particolare negli orari di accesso agli uffici da parte del pubblico esterno.
- Analogamente deve essere assicurata la custodia delle chiavi di locali, armadi e cassettiere in cui sono conservati i documenti contenenti dati personali e, in caso di furto o smarrimento, deve essere fatta pronta denuncia al responsabile.
- In caso di assenza dall'ufficio per cui il medesimo risulti 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.

. Nel corso del trattamento devono essere assunte adeguate misure e adottati appositi accorgimenti affinché i dati trattati non vengono portati alla conoscenza anche occasionale di soggetti terzi che si trovino nei luoghi in cui il trattamento è effettuato.

Il Responsabile

.....

Per ricevuta .....

Modena, .....