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.593 del 11/6/2004 e successive modificazioni

ultime modifiche approvate con delibera della Giunta Comunale

n.707 del 22/12/2015

SOMMARIO:

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 telematico alle banche dati

A) Il Trattamento dei dati con strumenti elettronici

1) Struttura del sistema e protezioni

1.1 Architettura della rete

L'Amministrazioni si è dotata di una rete in fibra ottica in proprietà, che collega oltre 40 sedi sul territorio comunale , a formare un anello, che consente il funzionamento della rete anche nel caso di guasto su una tratta di collegamento.

Su questa rete l'amministrazione veicola i servizi dati e di fonia interna , alcuni servizi sul territorio gestiti dal Comune (es. il sistema di telecamere di video sorveglianza), ed altri gestiti da Lepida SpA (wifi pubblico cittadino).

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 azienda

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
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 Protocol), 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 Active Directory utilizzato per autenticare gli utenti di risorse condivise su rete come:
    - cartelle
    - stampanti
    - applicativi su server web

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 al personal computer con sistema Windows XP e seguenti ci si avvale dei sistemi nativi di autenticazione sia tramite username e password definite come credenziali locali, cioè memorizzate sul pc stesso, sia tramite credenziali di dominio Active Directory se il pc è stato inserito nel dominio.

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 a cui compete la gestione del sistema informatico / telematico

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 che utilizzano i sistemi LDAP o Active Directory è il Responsabile dell'Ufficio Reti Informatiche del Settore a cui compete la gestione del sistema informatico / telematico 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, il Dirigente del Settore competente o il responsabile del trattamento dei dati da lui delegato richiede al preposto alla gestione , attraverso l'apposita procedura informatica , 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 nelle banche dati necessarie 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 avranno un resposabile incaricato della gestione

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 .

<u>Accesso ad applicazioni e banche dati del Settore di appartenenza</u>

Il Dirigente del Settore di appartenenza/ responsabile delegato sulla base dell'incarico conferito al lavoratore, comunica al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, 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 al preposto alla gestione, attraverso l'apposita procedura informatica, 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
Dopo 30 giorni dalla data di cessazione del rapporto lavorativo, il preposto alla gestione delle credenziali, attraverso una procedura automatica, ricava dalla Banca dati centralizzata del Settore a cui compete la gestione del personale, il nominativo del lavoratore cessato, ne revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica, e ne informail 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 a cui compete la gestione del personale, spetta al Dirigente del Settore competente/ responsabile delegato comunicare tempestivamente al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, 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, attraverso l'apposita procedura informatica, il Dirigente del Settore competente e il responsabile informatico dell'applicazione.

Prima della cessazione del rapporto di lavoro, il lavoratore deve eliminare i documenti e le e-mail che non siano di interesse del Settore, autorizzando attraverso l'apposita procedura informatica, 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 concordando con lui le modalità di gestione della stazione di lavoro e dei dati in essa contenuti.

Nel caso in cui, per esigenze contingenti, non sia stata rilasciata la liberatoria, il Dirigente di Settore/ responsabile delegato richiede ed autorizza l'intervento del tecnico dell'Ufficio reti Informatiche, che avverrà, ove possibile, alla presenza dell'interessato. Questo intervento verrà documentato mediante apposito verbale redatto a cura del Dirigente di Settore/ responsabile delegato , che ne informa l'interessato alla prima occasione utile, qualora non presente.

Nel caso in cui si provveda al ritiro della stazione di lavoro, i dati legati al profilo del lavoratore verranno resi indisponibili 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 a cui compete la gestione del personale , provvede a revocare tutte le autorizzazioni all'accesso del lavoratore, ad eccezione dell'indirizzo di posta elettronica, e ne informa, attraverso l'apposita procedura informatica, il responsabile informatico dell'applicazione. Su richiesta del Dirigente di Settore 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 e delle competenze a quest'ultimo attribuite, comunica al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, 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 e per le nuove abilitazioni procede con le modalità previste nel caso di nuova assunzione informando, attraverso l'apposita procedura informatica, 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 di interesse del Settore e successivamente a rimuoverli dalla propria stazione di lavoro. Su richiesta del Dirigente di Settore il lavoratore trasferito deve altresì reindirizzare al Settore di provenienza tutta la corrispondenza di posta elettronica di competenza di quest'ultimo.
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) che potrà essere modificato o integrato in relazione alle specifiche esigenze del Settore
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 al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, :

- 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 pari alla durata del contratto/ convenzione, se conosciuta. In caso contrario il periodo di validità delle credenziali è di dodici mesi . Almeno 60 giorni prima della scadenza il preposto alla gestione delle credenziali comunica al Dirigente di Settore tramite e.mail che, scaduto il periodo di validità, le credenziali dell'utente, salvo diversa comunicazione, saranno disabilitate. Trascorsi 30 giorni dalla scadenza del periodo di validità delle credenziali, senza che sia pervenuta una diversa comunicazione da parte del Dirigente di Settore, l'utente verrà dimissionato.

L'utente esterno che utilizza un PC di proprietà del Comune, prima della cessazione a qualsiasi titolo del suo incarico, deve eliminare dallo stesso 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 concordando con lui le modalità di gestione della stazione di lavoro e dei dati in essa contenuti. Nel caso in cui, per esigenze contingenti, non sia stata rilasciata la liberatoria, il Dirigente di Settore/ responsabile delegato richiede ed autorizza l'intervento del tecnico dell'Ufficio Reti Informatiche, che avverrà, ove possibile, alla presenza dell'interessato Questo intervento verrà documentato mediante apposito verbale redatto a cura del Dirigente di Settore/ responsabile delegato che ne informa il lavoratore alla prima occasione utile.qualora non presente

Nel caso in cui si provveda al ritiro della stazione di lavoro i dati legati al profilo dell'utente esterno verranno resi indisponibili 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 dell'utente esterno. Trascorso tale periodo il preposto provvederà alla eliminazione definitiva dei suddetti dati.

Accesso alle banche dati

L'accesso telematico alle banche dati del Comune di Modena 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 competente 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, sono identiche 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.
Sulle stazioni non definite nel dominio Active Directory viene creato un profilo con lo stesso userid che l'utente ha sui sistemi centralizzati di autenticazione ma con passwod provvisoria . Sulle stazioni definite in Active Directory il cambio di password è gestita automaticamente. Il dipendente ha l'obbligo di impostare la password seguendo la procedura di cambio password nel rispetto della normativa vigente.

Le password gestite tramite il sistema LDAP sono composte da 8 caratteri e scadono automaticamente 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 se la stazione di lavoro non è definita in dominio Active Directory. .

Qualora invece l'utente LDA*P* o l'utente la cui stazione di lavoro sia definita in Active Directory dimentichi la propria password, dovrà:

- rivolgersi al lavoratore da lui delegato (si veda paragrafo 3.3);

oppure:

- rivolgersi all'Ufficio Reti Informatiche che provvederà, previa identificazione personale, a fornire al lavoratore o a un suo delegato, una password provvisoria che consentirà di accedere alla procedura di modifica ed ottenere quella definitiva;

oppure:

- utilizzare l'apposita procedura informatica che consente di ottenere, tramite SMS inviato ad un cellulare precedentemente comunicato dal lavoratore, un codice d'accesso con cui ottenere una password provvisoria che consentirà poi di accedere alla procedura di modifica ed ottenere quella 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
Per riattivare le credenziali, l'utente dovrà rivolgersi all'Ufficio Reti Informatiche 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 Reti Informatiche del Settore a cui compete la gestione del sistema informatico / telematico del Comune, che provvederà alla designazione del personale incaricato.

3.2 Programmi antivirus

Su tutti i PC è installato un programma antivirus che viene aggiornato 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, sistema di filtraggio della navigazione e file server, ovvero server che permettono la condivisione di documenti.
I Server di Gestione Antivirus si aggiornano in modo automatico
Il software antivirus provvede automaticamente ad effettuare una scansione completa dei dischi interni delle stazioni di lavoro una volta alla settimana

3. 3 Interventi di accesso o manutenzione del PC

Richiesta di accesso

In caso di assenze programmate dal lavoro (per ferie o per qualsiasi altro motivo) il lavoratore attiva preventivamente il sistema di risposta automatica. Il messaggio di risposta predefinito deve essere personalizzato dall'utente e potrà indicare l'indirizzo di posta elettronica di un altro utente al quale il mittente può fare riferimento in caso di comunicazioni urgenti.

In caso di assenze dal lavoro non programmate, l'utente attiva da remoto, se possibile, il sistema di risposta automatica della propria casella di posta elettronica.

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 il Dirigente di Settore, sulla base delle scelte operative/organizzative effettuate, valuta i casi in cui il 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 Reti Informatiche , 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 Reti Informatiche 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 a cui compete la gestione del sistema informatico / telematico nomina la società che effettua la manutenzione dei sistemi hardware o software responsabile del trattamento dei dati utilizzando l'allegato modello 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 Reti informatiche 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 a cui compete la gestione del sistema informatico / telematico, all'inizio della collaborazione l'elenco degli incaricati al trattamento e successive variazioni

f) trasmettere al Dirigente del Settore a cui compete la gestione del sistema informatico / telematico il nominativo degli amministratori di sistema affinchè si possa provvedere al loro incarico

Il Dirigente del Settore a cui compete la gestione del sistema informatico / telematico nomina altresì gli amministratori di sistema tra quelli indicati dalla società, previa valutazione , da parte del Responsabile del Servizio Progetti telematici, Comunicazione e Città intelligente, delle caratteristiche di esperienza, capacità e affidabilità desunte dai relativi curricula

3.5 Dismissione delle stazioni di lavoro

In caso di dismissione di PC, il Dirigente che ha in carico la stazione di lavoro deve prontamente 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) <u>Salvataggio dei dati</u>

Il salvataggio delle banche dati esistenti sui server è in carico all'Ufficio Reti Informatiche
Sui sistemi centralizzati vengono fatte copie almeno 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 una libreria di backup e di disaster recovery presso la sede della Polizia Municipale.
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 di interesse settoriale residenti solo sul singolo PC (escludendo pertanto, ad esempio, le banche dati che il lavoratore ha creato ad uso proprio, quelle di cui esiste una copia cartacea ed in genere, quelle che è possibile ricostruire attingendo ad altre banche dati) vanno salvate su supporto elettronico a cura del lavoratore.
Spetta al Dirigente di Settore/ responsabile delegato effettuare la verifica periodica dell'effettivo salvataggio di questi dati e, eventualmente, richiedere all'Ufficio Reti Informatiche il supporto elettronico necessario. Tempi, modalità del salvataggio e di conservazione , sono definiti nelle istruzioni impartite al lavoratore dal Dirigente di Settore/ responsabile delegato, tenendo conto che la frequenza di salvataggio dovrà essere almeno settimanale, .

Le copie di salvataggio effettuate dai singoli utenti, possono essere archiviate o distrutte, ma in ogni caso non possono essere usate per la trasmissione dei dati all'esterno.

5) Locali

La sala macchine dell'Ufficio Reti Informatiche dove risiedono fisicamente i server e le librerie a dischi magnetici su cui sono memorizzati i dati dell'Ente, è dotata di impiantistica tale da garantire la sicurezza fisica dell'hardware, sia delle banche dati:

1. porta d'ingresso ad accesso controllato da videocitofono;
2. stabilizzatore di temperatura per i locali;
3. gruppo elettrogeno esterno e doppio gruppo di continuità e di stabilizzazione della corrente;
4. impianto di rilevamento fumi e spegnimento automatico in caso di

incendio, collegato con la sede di una società di sicurezza e pronto intervento;
5.impianto antintrusione collegato con la sede di una società di sicurezza e pronto intervento.

La sala macchine secondaria di Disaster Recovery sita presso la sede della Polizia Municipale in cui risiede la libreria a dischi magnetici utilizzata per le copie di backup, è dotata di:

1. porta d'ingresso al locale e sistema di videosorveglianza controllato dalla centrale operativa PP.MM.
2. stabilizzatore di temperatura per i locali;
3. gruppo elettrogeno esterno e gruppo di continuità e di stabilizzazione della corrente.

6) Cautele generali

6.1 Password

Il sistema centralizzato di autenticazione LDAP provvede in modo automatico alla scadenza trimestrale della password

Nel caso in cui le password siano impostate dall'utente , è sua responsabilità provvedere alla loro modifica almeno ogni tre mesi.

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.**

6.2 Uso del Computer

Il PC non deve essere lasciato incustodito.
In caso di assenza anche temporanea dall'ufficio, l'utente attivo al momento deve essere disconnesso o deve essere attivata la modalità salvaschermo con protezione mediante password
Il Dirigente di Settore/ responsabile delegato può impartire ulteriori istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro.

6.3. Custodia dei supporti

Devono essere impartite, da parte del Dirigente di Settore/ responsabile delegato, le istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati per motivi di sicurezza e 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 Comunicazione e Città intelligente
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 Comunicazione e Città intelligente
4	Banca dati residente su supporti di memorizzazione non in linea (CD ROM, DVD, chiave USB ….)	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, Patrimonio e Manutenzione urbana 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 Lavori Pubblici, Patrimonio e manutenzione urbana . 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 Lavori Pubblici, Patrimonio e manutenzione urbana cura la gestione dei sistemi di allarme esistenti nei palazzi di Via Galaverna 8, Via Santi 40, Via Santi 60 , Via Costa 13 .

5. I Servizi a cui compete la gestione del sistema informatico / telematico 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 a cui compete la gestione del personale dovrà curare la formazione 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..

Ogni Settore dovrà curare la formazione dei propri dipendenti avvalendosi, se lo ritiene opportuno, della collaborazione dell'ufficio che si occupa dell'organizzazione dell'attività formativa

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.

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 la Rete civica l'adozione delle misure più opportune alla 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 a cui compete la gestione del sistema informatico / telematico 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.

Nel caso in cui l'amministratore di sistema appartenga ad un altro Settore, fatta salva una diversa pattuizione, la designazione da parte del Dirigente del Settore a cui compete la gestione del sistema informatico / telematico avviene previa richiesta del Dirigente del Settore di appartenenza che ne attesta le caratteristiche di esperienza, capacità e affidabilità.

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 a cui compete la gestione del sistema informatico / telematico 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 a cui compete la gestione del sistema informatico / telematico 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 a cui compete la gestione del sistema informatico / telematico

- 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 telematico alle banche dati

ALLEGATO A1)

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 e successive modifiche ed integrazioni;

- *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;

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.
Il preposto alla gestione delle credenziali imposta per l'utente un periodo massimo di validità pari alla durata del contratto/ convenzione, se conosciuta. In caso contrario il periodo di validità delle credenziali è di dodici mesi . Almeno 60 giorni prima della scadenza il preposto alla gestione delle credenziali comunica al Dirigente di Settore tramite e.mail che, scaduto il periodo di validità, le credenziali dell'utente, salvo diversa comunicazione, saranno disabilitate. Trascorsi 30 giorni dalla scadenza del periodo di validità delle credenziali, senza che sia pervenuta una diversa comunicazione da parte del Dirigente di Settore, l'utente verrà dimissionato.

Devono altresì essere rispettati, per quanto compatibili, gli obblighi di condotta previsti dal Codice di comportamento del Comune di Modena

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) .....

ALLEGATO A2)

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.*

Devono altresì essere rispettati per quanto compatibili, gli obblighi di condotta previsti dal Codice di comportamento del Comune di Modena

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	Comunicazione 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.

ALLEGATO C)

CONVENZIONE PER L'ACCESSO TELEMATICO ALLE BANCHE DATI

CONVENZIONE TRA IL COMUNE DI MODENA E ..... PER L'ACCESSO TELEMATICO ALLA BANCA DATI .....

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

e

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

- vista la nota del ..... pervenuta al protocollo generale in data ..... n..... con la quale ..... ha chiesto di aderire alla convenzione che consente l'accesso alla banca dati .....essenziale per lo svolgimento dei propri compiti istituzionali, specificando gli titolano l'Ente all'accesso dei dati**;**
-
- valutata la legittimità della richiesta in considerazione delle motivazioni di pubblica utilità rappresentate;
-
- vista la propria determinazione n. ..... del ..... con la quale si è ritenuto di addivenire alla stipula della convenzione; adempimenti normativi, le finalità istituzionali perseguite e i motivi che

- richiamata la delibera della Giunta Comunale n..... del ..... con cui è stato definito lo schema di convenzione per l'accesso alle banche dati

Visti *(nella convenzione andranno inserite le leggi di riferimento):*

- .....
- .....
- .....
- 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 Oggetto della convenzione

Il Comune autorizza l'accesso alla banca dati informatizzata degli archivi …..... per le specifiche finalità istituzionali indicate nella richiesta secondo le modalità e nei limiti specificati nei successivi articoli.
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 ….....
L'accesso a dati ulteriori rispetto a quelli ai quali viene consentito l'accesso con la presente convenzione potrà essere autorizzato 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.2 – Utilizzo dei dati

L'Ente si impegna a:
- utilizzare le informazioni acquisite dal titolare esclusivamente per le finalità dichiarate, nel rispetto della normativa vigente, anche in materia di consultazione delle banche dati, osservando le misure di sicurezza ed i vincoli di riservatezza previsti dal Codice della Privacy;
- procedere al trattamento dei dati personali, in particolare di quelli sensibili e giudiziari, osservando le misure di sicurezza ed i vincoli di riservatezza previsti dal Codice della Privacy rispettando i canoni di pertinenza e non eccedenza nel trattamento delle informazioni acquisite nonché di indispensabilità per i dati sensibili e giudiziari ;
- garantire che non si verifichino divulgazioni, comunicazioni, cessioni a terzi, né in alcun modo riproduzioni dei dati nei casi diversi da quelli previsti dalla legge, provvedendo ad impartire, ai sensi dell'art. 30 del Codice della Privacy, precise e dettagliate istruzioni agli incaricati del trattamento, richiamando la loro attenzione sulle responsabilità connesse all'uso illegittimo dei dati;
- non duplicare i dati resi disponibili e non creare autonome banche dati non conformi alle finalità per le quali è stato autorizzato l'accesso;
- garantire che l'accesso ai dati verrà consentito esclusivamente a personale o assimilati ovvero a soggetti che siano stati designati dall'Ente fruitore quali incaricati o responsabili esterni del trattamento dei dati, procedendo, anche con apposite verifiche almeno trimestrali, alla tempestiva comunicazione al Comune della revisione del profilo di abilitazione e alla disabilitazione dei soggetti proposti ad altre mansioni o che abbiano cessato il rapporto di lavoro con l'Ente ;
- cancellare i dati ricevuti dal titolare non appena siano state utilizzate le

informazioni secondo le finalità dichiarate;
- formare gli utenti abilitati sulle specifiche caratteristiche, proprietà e limiti del sistema utilizzato per l'accesso ai dati e controllarne il corretto utilizzo.
- garantire l'adozione al proprio interno delle regole di sicurezza atte ad adottare procedure di registrazione che prevedano il riconoscimento diretto e l'identificazione certa dell'utente e adottare regole di gestione delle credenziali di autenticazione e modalità che ne assicurino adeguati livelli di sicurezza . Nel caso le credenziali siano costituite da una coppia username/password, devono essere previste politiche di gestione della password che rispettino le misure minime di sicurezza previste dal Codice della Privacy e la procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali da meccanismi crittografici di robustezza adeguata.
- utilizzare i sistemi di accesso ai dati in consultazione on line esclusivamente secondo le modalità con cui sono stati resi disponibili e, di conseguenza, a non estrarre i dati per via automatica e massiva (attraverso ad esempio i cosiddetti"robot") allo scopo di velocizzare le attività e creare autonome banche dati non conformi alle finalità per le quali è stato autorizzato all'accesso;
- comunicare tempestivamente e comunque entro 24 ore dalla conoscenza del fatto all'amministrazione titolare :

- eventuali incidenti sulla sicurezza occorsi al proprio sistema di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza ;
- ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;
- ogni modificazione tecnica e/o organizzativa del proprio dominio, che comporti l'impossibilità di garantire l'applicazione delle regole di sopra riportate e/o la loro perdita di efficacia
- 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
- garantire, in caso di cooperazione applicativa, che i servizi resi disponibili verranno esclusivamente integrati con il proprio sistema informativo e non saranno resi disponibili a terzi né direttamente né indirettamente per via informatica,
- fornire, in caso di cooperazione applicativa, contestualmente ad ogni transazione, il codice identificativo dell'utenza che ha posto in essere l'operazione. Il codice identificativo deve essere riferito univocamente al singolo utente. Laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato direttamente identificabile) dovrà in ogni caso essere garantita al Comune la possibilità, su richiesta, di identificare l'utente nei casi in cui ciò sia necessario.
-

L'Ente si impegna altresì al rispetto, per quanto compatibili, degli obblighi di

condotta previsti dal Codice di comportamento del Comune di Modena

L'Ente dichiara di essere consapevole della possibilità di controlli da parte del Comune previsti dal Codice della privacy per verificare il rispetto dei vincoli di utilizzo dei servizi. Per l'espletamento di tali controlli, che potranno essere effettuati anche presso le sedi del fruitore dove viene utilizzato il servizio, l'Ente si impegna a fornire ogni necessaria collaborazione

Art. 3 – Modalità di accesso e servizi erogati

Il Comune consente l'accesso telematico tramite la cooperazione applicativa/ la rete internet/ il trasferimento di dati attraverso file/ la posta elettronica certificata *(nella convenzione dovranno essere indicate le possibili opzioni tra le modalità di accesso sopra indicate o altre eventualmente individuate)* ai servizi di ricerca/ consultazione/ scaricamento dei dati/ altro *(nella convenzione dovranno essere individuate le possibili opzioni tra quelle indicate o altre eventualmente individuate).*
La descrizione dell'infrastruttura tecnologica resa disponibile per l'accesso ai dati, le modalità di fruizione dei dati e le regole di accesso, i livelli di servizio forniti, le regole minime di sicurezza sono contenute nell'allegato 1 che costituisce parte integrante della presente convenzione.

Art. 4 – Titolarità della banca dati

Il Comune conserva la piena ed esclusiva proprietà delle informazioni contenute nella banca dati ……. 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 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 posta elettronica certificata.

Art. 5 – Designazione responsabili

L'Ente individua come supervisore preposto all'individuazzione degli utenti e dei profili ……..
L'Ente individua come responsabile del trattamento ……. 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.
Il responsabile del trattamento si impegna a nominare gli incaricati del trattamento sulla base dello schema di incarico di cui all'allegato 3.
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.
Il supervisore risponde del controllo sulla gestione delle utenze
*I*n caso di gestione diretta delle utenze da parte del fruitore L'Ente individua altresì come soggetto deputato alla materiale amministrazione delle utenze ….....
L'Ente si impegna, qualora intenda avvalersi di soggetti terzi per realizzare servizi di interscambio, a darne comunicazione al Comune previa apposita designazione del soggetto delegato

Art. 6 – 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 …..... del Comune nonché per i danni derivanti da interruzioni, ritardi o errori nella elaborazione e/o trasmissione dei dati, ovunque si verifichino, 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.7- Costi

La convenzione non ha oneri economici salvo che per elaborazioni aggiuntive. Rimangono a carico dell'Ente i costi derivanti dalla connessione a Internet *(da inserire in convenzione se l'accesso avviene attraverso internet)* e i costi derivanti dalla realizzazione dell'infrastruttura di collegamento con il Comune (connessione a Internet o altro)

Art.8 - Durata

La presente convenzione avrà durata di …..... anni dalla data di sottoscrizione con possibilità di rinnovo esplicito per altri …..... anni.
Il Comune si riserva la possibilità di recedere in qualsiasi momento dalla presente convenzione a suo insindacabile giudizio, previa comunicazione inviata con posta elettronica certificata , con un preavviso di 15 giorni lavorativi 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.9 – Foro competente

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

Art.10 - 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 e è esente da imposta di bollo ai sensi dell'art.16 – Tabella allegato B – del DPR 642/72.

Art. 11 – Spese contrattuali

Non sono previste spese contrattuali.

Art. 12 – Informativa

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

Modena, ...

allegato 1

Criteri tecnici per le modalità di accesso ai dati

Glossario

Accesso telematico: la possibilità che soggetti esterni all'amministrazione titolare accedano a specifici dati attraverso una rete telematica.
Comune: l'amministrazione titolare della banca dati che mette a disposizione i relativi servizi di accesso sulla base della convenzione predisposta in ottemperanza a quanto previsto dall'art.58 comma 2 del Codice dell'Amministrazione Digitale.
Ente: l'amministrazione che accede ai dati resi disponibili dal Comune, secondo le regole e con le modalità definite nella convenzione a cui l'ente aderisce
Banca dati : l'insieme di dati omogenei, memorizzati in uno o più archivi informatici, organizzati e resi accessibili mediante uno strumento software.
Cooperazione applicativa: la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'interazione dei metadati, delle informazioni e dei procedimenti amministrativi
Posta elettronica certificata: il sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili
Disponibilità dei dati: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge.

Ricerca dei dati : la possibilità di individuare l'esistenza di dati in base al contenuto di metadati corrispondenti

Consultazione dei dati: la possibilità di accedere ai dati 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

Scaricamento (fruibilità) dei dati: la possibilità di trasferire i dati nei sistemi informativi automatizzati di un'altra amministrazione o ente. Il trasferimento del dato non ne modifica la titolarità.

(Inserire nella convenzione l'eventuale elencazione e definizione dei documenti informatici a cui si accede)

Descrizione dell'infrastruttura tecnologica resa disponibile per l'accesso ai dati

L'accesso ai dati è reso disponibile attraverso il Sistema pubblico di connettività / altra infrastruttura (*A seconda della tipologia di dati a cui si chiede l'accesso va indicata l'infrastruttura tecnologica utilizzata)*

Modalità di accesso telematico e regole di accesso

L'accesso telematico alla banca dati informatizzata degli archivi …..... è consentita tramite la cooperazione applicativa/ la rete internet/ il trasferimento di dati attraverso file/ la posta elettronica certificata. *(A seconda della tipologia di dati vanno indicate le possibili opzioni tra le modalità di accesso sopra indicate o altre eventualmente individuate. La scelta della modalità del trasferimento attraverso file deve essere adeguatamente motivata).*

Il supervisore è tenuto a comunicare al Comune entro ….. 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

Il numero massimo di utenti abilitati è di …..

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.

Alla banca dati potranno accedere esclusivamente gli incaricati dotati delle proprie credenziali d'accesso.

Al fine di consentire lo svolgimento dell'attività di accesso alla banca dati, il Comune si impegna a fornire in busta chiusa ad ognuno dei suddetti operatori la password provvisoria separatamente dal codice di identficazione (userid)

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

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 supervisore e 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, con l'attribuzione dei relativi profili di autorizzazione , dando altresì conferma del permanere delle finalità e delle motivazioni per cui è stato concesso l'accesso alla banca dati .
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.

Regole minime di sicurezza

L'Ente si impegna a dare disposizioni ai propri utenti affinchè la password sia mantenuta segreta, venga conservata adeguatamente e 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.
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 assicura che l'accesso alla banca dati avvenga solo attaverso postazioni di lavoro connesse alla rete Ip o dotate di certificazione digitale che identifichi univocamente la postazione di lavoro nei confronti del Comune
Al fine di consentire agli operatori l'accesso alle sole informazioni pertinenti e non eccedenti rispetto al proprio profilo e alla finalità istituzionale perseguita dalla convenzione stessa, l'accesso ai dati sarà consentito attraverso la segmentazione degli stessi *(frase da inserire nell'allegato qualora si reputi necessaria la profilazione degli accessi)*
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, di mettere i file a disposizione dell'autorità giudiziaria, qualora vengano richiesti, nonché di effettuare periodici controlli che verranno eseguiti con le seguenti modalità: …..

La registrazione degli accessi verrà conservata per un periodo di tempo di …..
Nel caso vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), l'Ente deve in ogni caso garantire al Comune, a richiesta, di poter identificare l'utente nei casi in cui ciò si renda necessario
L'Ente dichiara che le modalità con cui verranno trattati i dati durante il loro ciclo di vita sono le seguenti: …..
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.
Periodici controlli potranno essere effettuati dal Garante della privacy, con l'eventuale supporto del Comune, in merito all'uso dei dati da parte dell'Ente.

Servizi forniti
I servizi erogati sono i seguenti: ricerca/ consultazione/ scaricamento/ altro *(indicare i servizi forniti sulla base di quanto concordato con l'Ente)*
Qualora l'Ente abbia necessità di disporre di elenchi di dati si procederà con le seguenti modalità:.....

Livelli di servizio
Il servizio avverrà con le seguenti modalità: …....
In caso di interruzioni programmate il Comune informerà attraverso la posta elettronica gli operatori interessati dei tempi previsti di interruzione e del ripristino del servizio.
Gli orari in cui il servizio di assistenza è operativo sono i seguenti: …..... In caso di malfunzionamento nell'accesso dei dati l'Ente potrà rivolgersi a ….....

Periodicità dell'aggiornamento dei dati
I dati oggetto di accesso sono aggiornati ogni.....

allegato 2

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 e successive modifiche ed integrazioni;

· la convenzione stipulata in data .....;

· 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;

Devono altresì essere rispettatti per quanto compatibili, gli obblighi di condotta previsti dal Codice di comportamento del Comune di Modena

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.
Il preposto alla gestione delle credenziali imposta per l'utente un periodo massimo di validità pari alla durata del contratto/ convenzione, se conosciuta. In caso contrario il periodo di validità delle credenziali è di dodici mesi . Almeno 60 giorni prima della scadenza il preposto alla gestione delle credenziali comunica al Dirigente di Settore tramite e.mail che, scaduto il periodo di validità, le credenziali dell'utente, salvo diversa comunicazione, saranno disabilitate. Trascorsi 30 giorni dalla scadenza del periodo di validità delle credenziali, senza che sia pervenuta una diversa comunicazione da parte del Dirigente di Settore, l'utente verrà dimissionato.

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) .....

allegato 3

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. In caso di allontanamento temporaneo dal terminale, la sessione deve essere bloccata anche attraverso eventuali meccanismi di time out
· 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.

Devono altresì essere rispettatti per quanto compatibili, gli obblighi di condotta previsti dal Codice di comportamento del Comune di Modena

Il Responsabile
….....

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