

Comune di Modena

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

DECRETO LEGISLATIVO 196/2003
(allegato B)

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

A) Il Trattamento dei dati con strumenti elettronici

1) Struttura del sistema e protezioni

1.1 Architettura della rete

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

Tutte le Sedi comunali (circa 30), ed alcuni servizi sul territorio gestiti dal Comune (parcheggi, 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 alla rete Internet ed alle reti di altri Enti mediante un sistema di firewall composto da due apparecchiature HW identiche, interconnesse tra loro, di cui una principale in produzione ed una di failover, normalmente in stand-by, pronta ad entrare in funzione nel caso in cui il firewall principale, per un motivo qualsiasi, interrompa il suo funzionamento.

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

Il sistema di firewall installato permette di gestire, tramite la definizione di DMZ (zone demilitarizzate), diverse politiche di sicurezza.

Per permettere l'accesso ad utenti non collegati in modo permanente alla propria rete (uffici periferici o di altri Enti), il Comune di Modena dispone di un Access Server, a cui è connesso un accesso primario ISDN Telecom, che è in grado di rispondere contemporaneamente a più telefonate, provenienti da apparati analogici (PSTN) o digitali (ISDN).

L'utente che chiede l'accesso deve identificarsi tramite utente/password; (per le modalità di assegnazione delle credenziali vedasi punti 2.3 e 2.4); dove possibile l'accesso è pure vincolato al numero di telefono chiamante.

L'Access-Server è connesso al firewall, che consente l'accesso a servizi diversi a

seconda dell'utente che si è autenticato.

Un secondo firewall è utilizzato per il controllo dei collegamenti sulla rete Provinciale e Regionale, e su reti dedicate.

In alternativa al collegamento su linea telefonica tramite access-server è stata attivata una modalità di collegamento tramite internet attraverso l'uso di VPN.

L'utente deve preventivamente installare sul proprio computer un software specifico fornito dal Comune di Modena, quindi autenticarsi tramite userid e password.

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, 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 NT4 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 NT4

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.

Sui personal computer con sistema Windows 98, che nativamente non è protetto da password, è stato installato un software che consente l'accesso con password, garantendo una relativa sicurezza.

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 NT4.

Questa autenticazione avviene in modo trasparente per l'utente (senza la richiesta di ulteriori autenticazioni) se le credenziali di accesso al PC (se Windows 2000 o superiore) sono le stesse che nel dominio NT4.

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.

Può accadere che, per esigenze di servizio, esistano stazioni di lavoro le cui credenziali di accesso non siano legate a un singolo dipendente, ma siano condivise da tutto un gruppo di operatori. Questa verifica sarà a carico del Dirigente a cui afferiscono gli operatori o del Responsabile del trattamento da lui designato

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.

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 richieste ed informa per iscritto, anche via e.mail, il responsabile informatico dell'applicazione .

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

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 Dirigente di Settore ed 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 procederà come nel caso indicato al paragrafo precedente.

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 al quale può richiedere, entro un mese, il recupero delle banche dati residenti sul PC e delle e-mail giacenti nella casella di posta disabilitata. Trascorso tale periodo il preposto provvederà alla pulizia dei dati rimasti sulla stazione di lavoro, prima della assegnazione ad altro 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 Dirigente di Settore ed 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 alle quali il lavoratore è autorizzato ad accedere. Il preposto alla gestione delle credenziali disabilita le autorizzazioni all'accesso da revocare, abilita il lavoratore alle banche dati richieste e ne informa per iscritto, anche via e.mail, il Dirigente di Settore ed il responsabile informatico dell'applicazione. Nel caso che il lavoratore necessiti di accedere a banche dati di un altro Settore, si procederà con le modalità previste nel caso di nuova assunzione.

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.

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

L'autorizzazione all'accesso dovrà essere preceduta dalla nomina del soggetto esterno

a 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 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 disabilite. 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 disabilite 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.

2.5 Modalità di gestione delle password

Le password utilizzate nei sistemi di autenticazione LDAP e NT4 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 NT4.

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 NT4 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

Il lavoratore, qualora dimentichi la password di accesso al proprio PC dovrà rivolgersi al servizio di assistenza che si recherà sul posto e consentirà all'utente l'accesso al PC solo allo scopo di impostare una nuova password

Qualora invece l'utente LDAP dimentichi la propria password o la faccia scadere senza sostituirla, dovrà recarsi presso l'Ufficio Sistema e Reti che provvederà, previa identificazione, a fornire in busta chiusa una password provvisoria che consentirà di accedere alla procedura di autenticazione ma che dovrà poi essere immediatamente sostituita da una nuova.

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 e non deve in alcun modo comunicarle a persone diverse od altri incaricati; qualora avesse il timore che la propria password sia divenuta di conoscenza di altri soggetti deve prontamente provvedere a modificarla.

2.6 Disattivazione credenziali per disuso.

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

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.

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

Se, in caso di assenza o impedimento del lavoratore, si rende indispensabile e indifferibile intervenire, per esclusiva necessità di operatività o sicurezza, sul PC in dotazione, 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 e comunicato al Dirigente Responsabile del Settore richiedente e, per conoscenza, al lavoratore da parte del Responsabile dell'Ufficio Sistema e Reti.

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. Ciò consente ai singoli settori di non istituire il registro delle password individuali.

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

Le società che effettuino manutenzione dei sistemi hardware o software sono considerate responsabili dei dati e devono, a tale scopo, rispettare le seguenti cautele:

- 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) eventuali interventi remoti di assistenza mediante collegamento devono essere preventivamente autorizzati dai tecnici dell'Ufficio Sistema e Reti che dovranno essere, altresì, avvisati al termine delle operazioni.
- d) sottoscrivere impegno formale al rispetto di tutte le norme e del presente documento.
- e) usare riservatezza su dati ed informazioni addivenuti in loro possesso.

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 magnetico o ottico 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 magnetico 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:

- a.chiusura di sicurezza per la porta di ingresso ai locali, ed accesso controllato da videocitofono per i dipendenti autorizzati;
- b.stabilizzatore di temperatura per i locali;
- c.gruppo di continuità e di stabilizzazione della corrente;
- d.cassaforte ignifuga per cassette, dischetti e CD di salvataggio;
- e.impianto di rilevamento fumi e spegnimento automatico in caso di incendio, collegato con la sede di una società di sicurezza e pronto intervento;
- f.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:
g.chiusura di sicurezza per la porta di ingresso al locale;
h.stabilizzatore di temperatura per i locali;
i.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 tra cui:

- per quanto concerne i dati sensibili e giudiziari contenuti in elenchi, registri, banche dati tenuti con l'ausilio di strumenti elettronici, l'adozione di tecniche di cifratura, codici identificativi o soluzioni analoghe che li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità;

- per quanto concerne i dati idonei a rivelare lo stato di salute e la vita sessuale, la loro conservazione separata dagli altri dati personali trattati per finalità che non richiedono il loro utilizzo nonché l'adozione di tecniche di cifratura, codici identificativi o soluzioni analoghe che li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità sia qualora essi siano trattati con strumenti elettronici, sia qualora siano contenuti in documenti cartacei (registri, elenchi.....)

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, Logistica e Manutenzione, 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 Servizio TecnicoManutentivo. 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 Servizio Tecnico Manutentivo 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 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. I Servizi Progetti Telematici e Sistemi e Reti stanno elaborando un piano per individuare i criteri da adottare per la cifratura dei dati personali dell'interessato idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24 dell'allegato b al codice 196/03 o per la separazione di tali dati dagli altri dati personali dell'interessato e stanno procedendo alla loro sperimentazione

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 del Settore Cultura, Sport, Turismo, Marketing e Politiche Giovanili 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.

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 risulta 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	organizzativa	incaricati

	assenza dell'incaricato)		
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

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.462 del 24/7/2007 come modificato ed integrato con deliberazione 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;

-trasmettere all' amministrazione l'elenco degli incaricati del trattamento ;

-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.*

Dichiara inoltre di essere a conoscenza del fatto che 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 di dati (1)	Tipologia di Banca Dati /Archivi	Nome del Responsabile	Nome dell'incaricato	Codici (2) (3)	Ubicazione e 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.