ORIGINALE

C O M U N E D I B I B B I E N A

(P r o v i n c i a d i A r e z z o)

D E L I B E R A Z I O N E D I G I U N T A C O M U N A L E

N. 34 **DEL 16/02/2011**

O G G E T T O:

AGGIORNAMENTO DOCUMENTO PROGRAMMATRICO SULLA SICUREZZA

Oggi, 16/02/2011 alle ore 10,00 ed in prosieguo nella sala delle adunanze della sede comunale, si e' riunita la Giunta Comunale.

Presiede la seduta il sig. BERNARDINI Daniele, nella sua qualità di Sindaco.

Fatto l'appello nominale risultano presenti ed assenti:

BERNARDINI Daniele	P	
CONTICINI Luca		A
CAPORALI Matteo	P	
NASSINI Renato	P	
PIANTINI Fabrizio	P	
PAPERINI Mara	P	
LORENZONI Federico	P	
	presenti	assenti
	6	1

Assiste il dott. Liberto Giuseppe, nella sua qualità di Segretario Comunale incaricato della redazione del verbale.

Il Presidente, constatato il numero legale degli intervenuti, invita i presenti alla trattazione dell'argomento indicato in oggetto.

ESECUZIONE IMMEDIATA SI

ALLEGATI SI

Proposta di deliberazione della Giunta comunale
Unità Organizzativa n. 1 – Affari generali

OGGETTO: AGGIORNAMENTO "DOCUMENTO PROGRAMMATICO SULLA SICUREZZA" DPS

Il Sindaco Sig. Bernardini Daniele;

Richiamate:
- la deliberazione di Consiglio Comunale n. 125 del 30.12.2005 di approvazione del Regolamento comunale per il trattamento dei dati sensibili;
- la deliberazione di Giunta Comunale n. 284 del 15.12.2005, modificata con deliberazione di Giunta comunale n. 69 del 21.03.2006, di approvazione del documento per la sicurezza dei dati sensibili;

Dato atto che con le deliberazioni sopra richiamate sono stati indicati:
- l'elenco dei trattamenti dei dati personali;
- l'analisi dei rischi che incombono sui dati e le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali ai fini della loro custodia e accessibilità;
- la disciplina del trattamento dati con strumenti elettronici e non;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- per i dati "sensibili" l'individuazione di criteri specifici di sicurezza;

Rilevato che l'efficacia delle misure di sicurezza deve essere oggetto di controlli periodici da eseguirsi con cadenza almeno annuale, ragion per cui il documento programmatico della sicurezza deve essere aggiornato entro il 31.03.2011, tenendo conto delle variazioni alla struttura organizzativa ed alla gestione operativa dei trattamenti;

Accertato che in fase istruttoria è stato acquisito il parere favorevole di regolarità tecnica, espresso ai sensi ed agli effetti dell'art. 49, comma 1, del D.Lgs. n. 267/2000, pareri allegati:

DELIBERA

1) di approvare, per le motivazioni indicate in premessa, il "Documento Programmatico sulla sicurezza" aggiornato;

LA GIUNTA COMUNALE

Esaminata la sopra riportata proposta di deliberazione;

Visto l'art. 48 del D.lgs 267/2000;

Recepiti i pareri di cui all'art. 49 del D.lgs 267/2000;

Visto il vigente Statuto Comunale;

Con voti unanimi favorevoli espressi palesemente;

D E L I B E R A

Di approvare la suestesa proposta di deliberazione che qui si intende integralmente riportata.

COMUNE di BIBBIENA

(Provincia di Arezzo)

Servizio: **AFFARI GENERALI**

OGGETTO DELLA DELIBERAZIONE
AGGIORNAMENTO DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

PARERE DI REGOLARITA' TECNICA

Il Responsabile del servizio interessato, ai sensi dell'art. 49, comma primo, del Decreto Legislativo 18/08/2000, n. 267 per quanto concerne la regolarità tecnica, esprime parere:

FAVOREVOLE

Bibbiena, 16/02/2011

IL RESPONSABILE DEL SERVIZIO
(D.ssa Ivana Vignoli)

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

Indice

Allegato alla deliberazione N° 34 del 16-02-2011

Il Segretario ~~Direttore~~ Generale
Dott. LIBERTO GIUSEPPE

1. Figure interessate: Titolare - Responsabile – Incaricato

La legge istituisce la figura del **Titolare** identificandola nella "persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza". Oltre al Titolare, il Codice prevede altre due figure, il Responsabile e gli Incaricati del trattamento, cui sono affidati compiti specifici volti a garantire il rispetto delle disposizioni di legge.
Il **Responsabile** è la persona preposta dal titolare al trattamento di dati personali.
Gli **Incaricati** sono le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal Titolare o dal Responsabile.

2. Organizzazione interna del Comune

Il Comune ha previsto una specifica organizzazione interna, articolata nel modo seguente, per individuare formalmente le figure previste dal Codice:
Titolare del trattamento dei dati è il Comune di Bibbiena, nella persona fisica del Sindaco
• il Titolare, nomina come Responsabili del trattamento i Responsabili di servizio
• I Responsabili provvedono a nominare Incaricati i collaboratori che, nello svolgimento della propria attività, svolgono operazioni nell'ambito del trattamento di propria competenza. Il Titolare, cui competono le decisioni in ordine alle finalità e modalità del trattamento ed alle relative misure di sicurezza, è responsabile di tutti gli adempimenti, non delegabili, relativi alle notificazioni al Garante, alle procedure d'autorizzazione da parte del Garante ed alla nomina dei Responsabili.
Il Titolare delega al Responsabile:

- l'informativa agli interessati;
- la nomina degli incaricati per trattamenti elettronici o diversi, che non siano stati nominati dal Titolare stesso;
- la richiesta di consenso agli interessati;
- le istruzioni agli incaricati per archivi cartacei;
- la gestione dell'accesso selezionato agli archivi cartacei e l'accesso controllato ove siano trattati dati sensibili;
- l'applicazione ed il rispetto delle misure di sicurezza;
- la conservazione di documenti contenenti riproduzioni di informazioni relative al trattamento dati sensibili;
- le autorizzazioni accesso trattamento dati sensibili e relativi aggiornamenti;
- le autorizzazioni agli incaricati per gli strumenti utilizzati per trattamenti di dati sensibili e relativi aggiornamenti.

3. Organizzazione Comunale a protezione dei dati

Il Comune di Bibbiena, nell'ambito della Politica per la Sicurezza comunale, intende considerare la protezione del proprio patrimonio di informazioni (su supporti sia cartacei sia informatici) elemento fondamentale per la tutela e la continuità della propria attività.
Rientrano in tale patrimonio i dati personali oggetto di specifiche misure di protezione. L'organizzazione comunale e gli strumenti operativi che sono stati adottati per garantire l'efficacia delle azioni di protezione del patrimonio informativo, si applicano quindi anche alle categorie di informazioni individuate dal Codice ed ai processi che ne regolano il trattamento.
La protezione del patrimonio informativo comunale è quindi un obiettivo di primario interesse. Pertanto per Comune di Bibbiena è stato predisposto un documento con lo scopo di descrivere la

protezione delle informazioni aziendali, denominato "Documento per la sicurezza dei dati sensibili" approvato in data 15.12.2005 e modificato in data21.03.2006.
E' stato inoltre designato l'amministratore di rete.

4. Definizione dei requisiti di sicurezza ai sensi del Codice

Il Codice ha per finalità garantire che "il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".
Il Comune di Bibbiena pertanto, seguendo le indicazioni in materia di protezione dei dati, ha svolto un'attività di analisi dei rischi che incombono sui dati aziendali.
I tre aspetti da considerare per la protezione dei dati sono:

Riservatezza	Garantisce che l'informazione sia resa disponibile solamente ai processi che la devono elaborare ed all'utilizzatore che ne è autorizzato all'uso.
Integrità	Garantisce che ogni informazione sia realmente quella originariamente immessa nel sistema informativo, ovvero successivamente legittimamente modificata.
Disponibilità	Garantisce la reperibilità delle informazioni in funzione delle esigenze di continuità dei processi comunali ed al fine del rispetto delle norme (di legge e non) che ne impongono la conservazione storica.

Tali requisiti forniscono un punto di partenza per l'identificazione dei possibili attacchi, individuabili in base all'analisi dello scenario effettuata e per la definizione dei criteri di protezione più efficaci.
Attraverso l'attività di audit periodico (promossa dal Titolare) viene verificata nel tempo l'efficacia delle misure adottate e la copertura del perimetro di intervento rispetto al complessivo patrimonio informativo. Tale attività permette di identificare le eventuali carenze nei sistemi di sicurezza, consentendo di migliorare l'analisi del rischio e le azioni correttive da intraprendere per correggere le problematiche riscontrate. La metodologia è stata applicata al perimetro costituito dai dati personali e sensibili il cui censimento è riportato nel Regolamento approvato con deliberazione di Consiglio Comunale n. 125/2005.

5. Perimetro per la valutazione delle vulnerabilità e dei rischi

L'individuazione delle vulnerabilità deriva da una fase di analisi della realtà comunale, sia per quanto riguarda l'architettura informatica, sia per l'individuazione degli eventuali trattamenti che prevedono l'impiego di contenitori/archivi di tipo cartaceo.
In base a quanto è possibile rilevare con questa metodologia vengono valutate le componenti potenzialmente soggette a rischio quali:

- reti e apparati di rete;
- elaboratori e software di sistema;
- software applicativo;
- supporti informatici di memorizzazione (per le attività dì reimpiego);
- infrastrutture;
- contenitori/archivi cartacei;
- archivi di Backup.

6. Criteri per la correzione delle vulnerabilità

Sulla base delle possibili vulnerabilità e delle necessità di protezione espresse, il Comune di Bibbiena individua la necessità di attuare un insieme di misure di protezione così classificabili:
Misure di tipo organizzativo, quali:

- le misure per l'assegnazione di compiti e responsabilità (nomine);
- le misure per l'aumento della sensibilità aziendale nei confronti delle tematiche di tutela dei dati (formazione);
- le misure per evitare l'attuazione di trattamenti di dati personali per finalità diverse da quelle autorizzate e consentite;
- le misure per la protezione di archivi cartacei e di supporti di memorizzazione.

Misure di protezione delle aree e dei locali (criteri di protezione fisica) e rispettive procedure, quali:

- le misure per la protezione dall'accesso intenzionale e non autorizzato ai locali e agli archivi (antintrusione);
- le misure per la protezione dei locali dall'accesso non autorizzato (intenzionale o non intenzionale) tramite le vie di accesso predisposte (controllo accesso);
- le misure per la protezione dei dati da eventi di origine naturale o dolosa (antincendio);
- le misure per la protezione da condizioni ambientali proibitive o da eventuali riduzioni dell'efficienza dei sistemi di supporto (impianti ausiliari).

Misure di protezione delle architetture di rete, degli applicativi e della trasmissione dei dati (criteri di **protezione logica** dei dati) e relative procedure quali:

- le misure per la protezione da accessi non autorizzati ad informazioni riservate (User Id, password, Screen Saver con password);
- le misure per la protezione da possibili danneggiamenti alle informazioni (antivirus);
- le misure per la protezione da eventuali perdite di disponibilità dei dati (backup differenziale giornaliero dei file server, mail server, application server con reimpiego di supporti di memorizzazione dopo azzeramento);
- le misure per la trasmissione sicura delle informazioni su rete;
- le misure per il trasferimento di dati mediante mezzi differenti dagli elaboratori (nell'utilizzo della POSTA, inviare buste sigillate, la cui integrità deve essere verificata dal ricevente; in caso di trasmissione via FAX, indicare mittente e destinatario, controllare il numero del destinatario e verificare che l'invio sia andato a buon fine; i documenti contenenti "dati sensibili" non devono essere trasmessi via fax).

7. Misure minime di sicurezza

Le **"misure minime di sicurezza"** previste sono state classificate nel modo seguente:
Trattamento informatico identificato dal codice (Mx) e dalla descrizione

- **M1** autenticazione informatica;
- **M2** adozione di procedure di gestione delle credenziali di autenticazione;
- **M3** utilizzazione di un sistema di autorizzazione;
- **M4** aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

- M5 protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- M6 adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- M7 tenuta di un aggiornato documento programmatico sulla sicurezza;
- M8 adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Trattamento non informatico

- M9 aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- M10 previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- M11 previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Sono poi state individuate le diverse tipologie di contesto, caratterizzate dai rispettivi contesti architetturali dalla tipologia di trattamento, e dalle misure di protezione in generale applicabili a ciascun contesto.

CONTESTO	MISURE DI PROTEZIONE
Trattamenti con strumenti elettronici	**M1, M2, M3, M4, M5, M6**
Trattamenti senza l'ausilio di strumenti elettronici	**M9, M10, M11**
Trattamenti con strumenti elettronici di dati sensibili o giudiziari	**M1, M2, M3, M4, M5, M6, M7**
Trattamenti di dati personali in ambito sanitario	**M1, M2, M3, M4, M5, M6, M7, M8**

8. Trattamenti con strumenti elettronici

Quanto previsto dal Disciplinare Tecnico (allegato B del D.Lgs. 196/03) è stato messo in corrispondenza alle misure minime di sicurezza in base alla tabella seguente.

Sistema di autenticazione informatica

Codice	*nr*	*Criterio*	*Conformità con la norma*
M1	1	Il trattamento di dati personali con strumenti elettronici è consentito agli Incaricati dotati di credenziali di autenticazione	conforme
M1	2	Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (user id) associato ad una parola chiave (password) riservata conosciuta solamente dal medesimo.	conforme
M2	3	Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.	conforme

M2	4	Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della password.	conforme
M1	5	La password, quando è prevista dal sistema di autenticazione, è composta da almeno 8 (otto) caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Le policy dell'azienda suggeriscono agli utenti di non utilizzare riferimenti facilmente riconducibili all'incaricato. La password viene assegnata all'incaricato ed è da lui modificata al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la password è modificata almeno ogni tre mesi.	conforme
M2	6	Lo user id non può essere assegnato ad altri Incaricati, neppure in tempi diversi.	conforme
M4	7	Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.	conforme
M4	8	Le credenziali sono disattivate anche in caso di perdita della qualità che consente all' incaricato l'accesso ai dati personali.	conforme
M2	9	Sono impartite istruzioni agli Incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento	conforme
M1	10	Il Titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.	conforme
M3	12	Quando per gli incaricati sono individuati profili dì autorizzazione di ambito diverso è utilizzato un sistema di autenticazione.	conforme
M3	13	I profili di autorizzazione, per ciascun incaricato o per classi omogenee di Incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare L'accesso ai soli dati necessari per effettuare le operazioni di trattamento.	conforme
M3	14	Periodicamente e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.	conforme

Altre misure di sicurezza

Codice	*nr*	*Criterio*	*Conformità con la norma*
M2	15	La lista dei profili di autorizzazione viene aggiornata almeno annualmente.	conforme
M5	16	I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinques del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.	conforme
M5	17	Gli aggiornamenti periodici dei programmi elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.	conforme.
M6	18	Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.	conforme

Documento Programmatico Sulla Sicurezza

Codice	*nr*	*Criterio*	*Conformità con la norma*
M7	19	Entro il 31 marzo di ogni anno, il Titolare del trattamento di dati sensibili o di dati giudiziari redige anche attraverso il Responsabile, se designato, un documento programmatico sulla sicurezza (DPS).	conforme

Ulteriore misure in caso di trattamento di dati sensibili

Codice	*nr*	*Criterio*	*Conformità con la norma*
M5	20	I dati sensibili o giudiziari di cui all'art.615-ter del codice penale sono protetti contro l'accesso abusivo, mediante l'utilizzo di idonei strumenti elettronici.	in corso di adeguamento
M6	21	Sono impartite 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.	conforme

M6	22	I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibile e tecnicamente in alcun modo riconoscibili.	conforme
M6	23	Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a 7 (sette) giorni.	conforme

Trattamenti senza l'ausilio di strumenti elettronici

Codice	*nr*	*Criterio*	*Conformità con la norma*
M9	27	Agli Incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia,per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.	in corso di adeguamento
M10	28	Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate.	in corso di adeguamento
M11	29	L'acceso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.	in corso di adeguamento

9. Misure per garantire accessibilità dei dati

Il Comune di Bibbiena si è dotato di procedure volte a garantire la continuità del servizio anche in caso di assenza dell'Incaricato al trattamento. Ovvero rendere disponibile gli strumenti elettronici cui l'incaricato ha accesso con credenziali di autenticazione (di seguito parola chiave). Ciò avviene nel rispetto dei requisiti di segretezza e non diffusione della parola chiave dell'Incaricato ed esclusivamente nei casi in cui l'assenza dell'Incaricato crei pregiudizio al Comune per servizi che esso deve garantire al proprio interno o verso utenti esterni.

10. La protezione fisica delle risorse

Gli uffici, a parte alcune eccezioni, sono generalmente presidiati nelle ore d'ufficio e vengono chiusi in caso di assenza di personale autorizzato.
Gli archivi cartacei presenti presso i diversi servizi di appartenenza dislocati nelle varie sedi del Comune necessitano di una revisione nella gestione della sicurezza e di una politica comune di regolamentazione degli accessi.
Il SIC, presente nella sede centrale del Comune risulta costantemente presidiato durante l'orario di lavoro.
Il locale è dotato di un unico ingresso ed è ventilato con sistema di condizionamento dell'aria. E' sprovvisto di sistema antincendio, antintrusione, antiallagamento. Il locale non è aperto al pubblico.

11. Obblighi di sicurezza per il Responsabile

Per quanto riguarda gli obblighi di sicurezza, si tratta di quanto previsto dalla legge e, quindi, delle misure minime descritte nel Disciplinare Tecnico.
In estrema sintesi:

1.	Il Responsabile identifica per iscritto gli incaricati del trattamento, cioè chi compie le operazioni (lettura,modifica,ricerca) sui dati.	Art.30,B.15
2.	Ogni Incaricato è dotato di un login individuale, assegnato sulla base di un profilo di autorizzazione che preveda l'accesso ai soli dati necessari allo svolgimento della propria attività	B.1, B.3, B 14
3.	Login e profili devono essere soggetti a revisione periodica, in modo che conservi l'accesso ai dati solo chi ne continua ad avere necessità o che abbia usato il login negli ultimi 6 mesi.	B.6,B7,B.8
4.	Al login è associato un sistema di autenticazione mediante password, token o biometrico.	B.2
5.	La password eventuale è lunga almeno 8 caratteri, è di qualità (non contiene riferimenti al login), è modificata almeno ogni 6 mesi, o 3 mesi in caso di trattamento di dati sensibili.	B.5
6.	Non è' prevista nessuna procedura di custodia delle password; l'amministratore della rete garantisce comunque l'accesso al dato in assenza dell'incaricato, tramite reset delle password stesse.	B.10
7.	Antivirus con aggiornamento almeno semestrale.	B.16
8.	Installazione di patch di sicurezza almeno annuale o semestrale per dati sensibili.	B.17
9.	Backup almeno settimanale dei dati (con disposizioni organizzative o automatismi tecnologici).	B.18
10.	Per i dati sensibili, sistemi antintrusione: firewall, IDS.	B20
11.	I supporti (nastri, cassette,floppy) contenenti dati sensibili devono avere norme di conservazioni particolari e devono essere cancellati prima del riutilizzo o distrutti.	B.21, B.22
12.	Il recovery dopo danneggiamento all'infrastruttura deve avvenire entro sette giorni.	B.23

Il Titolare adotta criteri per garantire che queste misure, e altre individuate sulla base dell'analisi dei rischi, vengano rispettate dai responsabili esterni. Gli accorgimenti adottati dal titolare nei confronti del Responsabile esterno sono clausole riportate nel documento di nomina formale. Il Titolare chiede evidenza di quanto il Responsabile esterno fa per adempire agli obblighi di legge.
Riprendendo la numerazione della tabella sopra riportata

1.	Il responsabile deve fornire al titolare l'elenco aggiornato degli incaricati del trattamento
2.	Non sono ammesse login collettive.
3.	Il responsabile deve fornire l'elenco di cui al punto 1. aggiornato periodicamente (cadenza almeno semestrale), descrivendo le modalità con cui controlla che i requisiti per l'accesso siano validi.
4.	Tipo di autenticazione adottato.
5.	Procedure di gestione dell'aggiornamento della password.
6.	Quanto adottato per garantire l'accesso ai dati (custodia delle password o possibilità di reset).
7.	Evidenza policy di aggiornamento antivirus. Rapporto periodico.
8.	Evidenza installazione patch di vulnerabilità. Rapporto periodico.
9.	Procedura o tecnologia adottata per il backup dei dati (al più settimanale).
10.	Descrizione dei meccanismi di protezione antintrusione adottati (IDS, firewall).
11.	Procedura di conservazione ed eventuale cancellazione /distruzione dei media con dati sensibili.

12.Programma di revisione ed adeguamento

Il presente documento verrà rivisto ed aggiornato almeno con cadenza annuale, a cura del Titolare, dopo aver controllato l'efficacia delle misure di sicurezza previste ed averle opportunamente adeguate.

Nelle revisioni del DPS, si terrà conto delle revisioni di politiche e linee guida (a livello istituzionale, metodologico, operativo e di controllo) in materia di protezione delle informazioni comunali, con particolare riguardo agli aspetti di sicurezza informatica.

OGGETTO: AGGIORNAMENTO DOCUMENTO PROGRAMMATRICO SULLA SICUREZZA

Letto e sottoscritto.

IL PRESIDENTE
D. BERNARDINI

IL SEGRETARIO
G. LIBERTO

CERTIFICATO DI PUBBLICAZIONE

La presente deliberazione e' pubblicata in data odierna, per rimanervi per 15 giorni consecutivi nel sito web istituzionale di questo Comune accessibile al pubblico (art. 32 c. 1 della legge 18 giugno 2009, n. 69) ed affissa all'Albo Pretorio e vi rimarrà per 15 giorni consecutivi, ai sensi e per gli effetti dell'art. 124 , comma 1 del D. Lgs. 18/08/2000, N. 267

N. 403 Reg. di Pubblicazione

Bibbiena, li' 25/02/2011

IL RESPONSABILE DELLA PUBBLICAZIONE
L. BOSCHI

COMUNICAZIONE AI CAPOGRUPPO

Prot. n. 4131 del 25/02/2011 ai sensi dell'art. 125 del D.Lgs. 18/08/2000, n. 267

CERTIFICATO DI AVVENUTA PUBBLICAZIONE

La presente deliberazione e' stata pubblicata in data **25/02/2011** per 15 giorni consecutivi fino al **12/03/2011** nel sito web istituzionale di questo Comune accessibile al pubblico (art. 32 c. 1 della legge 18 giugno 2009, n. 69) ed affissa all'Albo Pretorio per 15 giorni consecutivi, ai sensi e per gli effetti dell'art. 124 , comma 1 del D. Lgs. 18/08/2000, N. 267 e contro di essa non sono state presentate opposizioni.

Li'

N. 403 Reg. Pubb.

IL RESPONSABILE DELLA PUBBLICAZIONE

CERTIFICATO DI ESECUTIVITA'

Si certifica che la presente deliberazione è divenuta esecutiva il **08/03/2011** essendo strascorsi dieci giorni dall'inizio della pubblicazione, ai sensi dell'art. 134, comma 3, del D.Lgs. 18/08/2000, n. 267

-è stata pubblicata per 15 giorni consecutivi a partire dalla data suddetta sul sito web istituzionale di questo Comune e all'Albo Pretorio e che contro di essa non sono pervenute opposizioni

---

Bibbiena, lì _____

IL SEGRETARIO GENERALE