DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(Art. 34 DL.vo 196 del 30/06/2003)

in ottemperanza al disciplinare tecnico "allegato b"

al Decreto Legislativo 196/03

PREMESSA

Struttura informatica dell' Ente.

CAPITOLO I

Elenco dei trattamenti di dati personali e distribuzione dei compiti e delle responsabilità in relazione al trattamento dei dati.

CAPITOLO II

Analisi dei rischi e misure da adottare per garantire:

- integrità e disponibilità dei dati;
- protezione delle aree e dei locali.

CAPITOLO III

Criteri e modalità per il ripristino dei dati in caso di distruzione o danneggiamento.

CAPITOLO IV

PIANO DI FORMAZIONE AGLI INCARICATI DEL TRATTAMENTO:

- Conoscere i rischi;
- misure di prevenzione;
- profili normativi in relazione alle mansioni;
- responsabilità che ne derivano;
- modalità di aggiornamento sulle misure adottate dal Titolare.

CAPITOLO V

TRATTAMENTI ESTERNI: Criteri da adottare per garantire l'adozione delle misure minime di sicurezza.

CAPITOLO VI

Periodicità e modalità dei controlli.

PREMESSA

Struttura informatica dell' Ente

La struttura informatica dell' Ente è composta nel seguente modo:

- N° 1 server win 2000 server;
- N° 5 PC collegati in rete ubicati in 4 stanze;

Struttura della rete:

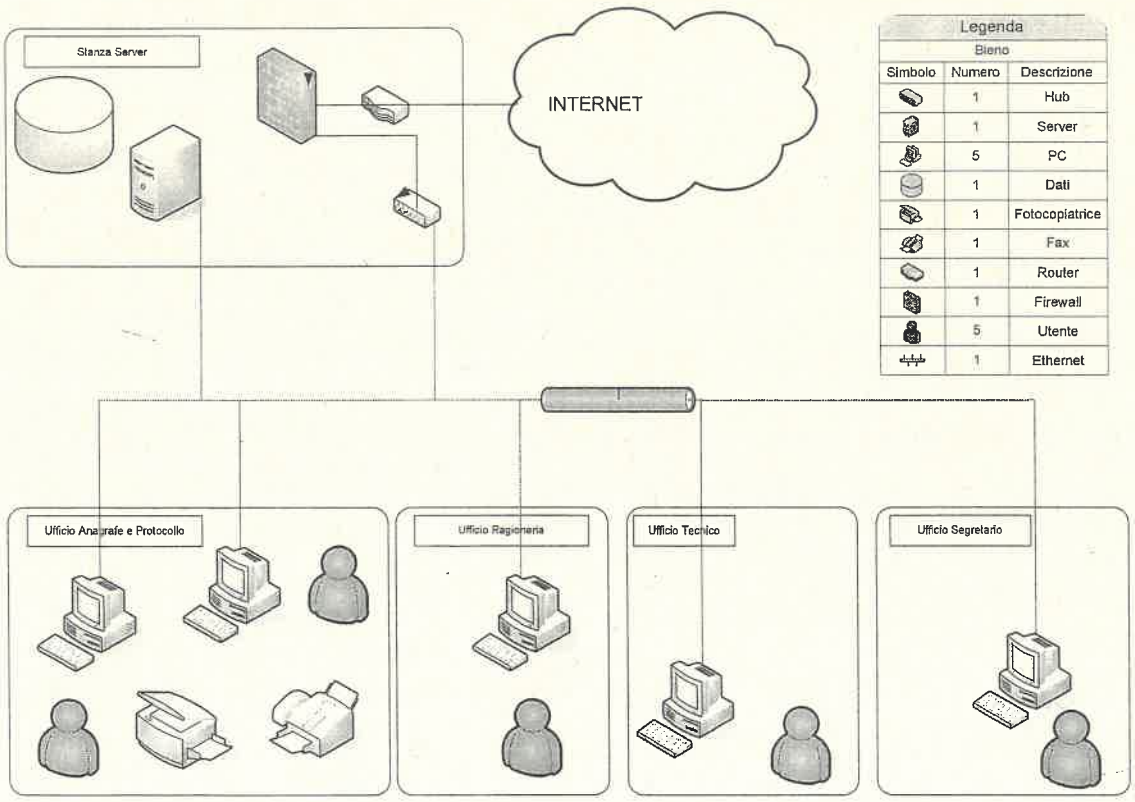
- LAN rete Ethernet a stella con hub situato nella stanza dove è ubicato anche il server;
- WAN collegamento ad Internet tramite router Adsl di proprietà di Informatica Trentina (tale router è dotato di firewall hardware configurato da Informatica Trentina);

Luogo di conservazione dei supporti informatici (Cassette, CD, floppy): ufficio Ragioneria;

Installazione di specifici programmi di back up: Ntbackup di Microsoft;

Nessuna installazione di specifici programmi di disaster recovery

Il presente documento e le misure di sicurezza indicate si riferiscono a tutti i dati contenuti nel sistema informatico del Comune di BIENO



CAPITOLO I

ELENCO DEI TRATTAMENTI DI DATI PERSONALI E RESPONSABILI IN RELAZIONE AL TRATTAMENTO DEI DATI:

Titolare del Trattamento: COMUNE DI BIENO
Responsabili dell' Ufficio: - vedi all. B
Responsabili del Trattamento interni: - vedi all. B
Responsabili del Trattamento esterni: - vedi all. B
Responsabili dei diritti dell'interessato: - vedi all. B
Custode delle password: - vedi all. B
Incaricati: - vedi all. B

Per ogni categoria di soggetti sopra esposti verrà allegato al presente documento copia della nomina contenente i compiti e le responsabilità in relazione al trattamento di dati.

AMBITO ED INCARICATI	TRATTAMENTO DI TUTTI I TIPI DI DATI PERSONALI	TRATTAMENTO DI DATI SENSIBILI E/O PENALI
1. Segreteria Generale e Contratti	A) a)Richieste accesso atti comunali; b)Archivio degli incarichi professionali del Comune; c)Archivio degli amministratori del Comune; d)Registro deposito atti giudiziari; e)Archivio ditte per gare d'appalto del Comune / LLPP e fornitura; f)Gestione dei contratti; g)Verbali delle deliberazioni di Giunta Comunale; h)Verbali delle deliberazioni di Consiglio Comunale; i)Raccolta determinazioni dirigenziali; j)Notificazioni messi comunali; Pubblicazioni atti.	A) a)Dati penali nella gestione degli archivi dei contratti (casellari giudiziali generali positivi);
2. Personale e organizzazione	A) a) Archivio dei dipendenti del Comune; b)dati modello 730; c)dati INPDAP; d)dati modello 770; e)dati modello 01/M; f)dati modello CUD; g)dati inquadramento contrattuale; h)archivio degli incarichi professionali e delle collaborazioni coordinate e continuative; i)archivio degli amministratori del Comune.	A) a)Dati sensibili e penali contenuti nei fascicoli personali dei dipendenti, dei collaboratori e degli amministratori; b)Dati sensibili e penali contenuti nelle buste paga, nelle denunce nominative e nei modelli 730, 770, CUD

3 Archivio e protocollo	A) a)Ordinanze per la tutela ambientale; b)ordinanze sindacali e dirigenziali; c)protocollo generale; d)archivio storico corrente; e) archivio rilevazione presenze del personale del Comune; f)Dichiarazioni ICI; g)numerazione civica;	A) a)Dati sensibili e/o penali eventualmente contenuti in documenti, certificati, ecc. che provengono a mezzo del servizio postale o sono presentati direttamente all'ufficio protocollo e che effettuata la protocollazione, sono trasmessi al responsabile della banca dati relativa alla pratica in trattazione; b)Dati sensibili e/o penali contenuti nelle ordinanze di cui l'ufficio detiene il registro cronologico e di cui custodisce la serie degli originali; c)Dati sensibili e/o penali contenuti in documentazione trasferita dall'ufficio competente all'archivio di deposito.
4 Servizi demografico/elettorali	A) a)Contratti cimiteriali; b)scritture private cimiteriali; c)Anagrafe della popolazione residente; d)pratiche immigrazione/emigrazione; e)cartellini carte d'identità; f)archivio elettorale; g)liste albi sezionali e generali degli elettori; h)archivio degli incarichi elettorali (presidenti, segretari, scrutatori di seggio); i)archivio italiani residenti all'estero; j)archivio dei cittadini stranieri (comunitari ed extracomunitari); k)archivio leva militare; l)registri degli atti di nascita/morte; m)stato civile.	A) a)Dati penali nelle informative da parte dell'autorità giudiziaria o uffici di PS per inibizione o sospensione carte d'identità valide per l'espatrio; b)dati penali nelle autorizzazioni del giudice tutelare ai genitori di minori separati o divorziati per rilascio delle carte d'identità valide per l'espatrio; c)dati sensibili e penali nelle pratiche di adozione minori; d)dati penali negli elenchi dei cittadini che hanno perso il diritto di voto.
5 Tributi	A) a)dichiarazioni ICIAP; b)dichiarazioni TOSAP; c)dichiarazioni TARSU.	A) a)Dati sensibili contenuti nei certificati medici acquisiti nell'ambito dei procedimenti dell'applicazione dei benefici TARSU e ICI.
6 Segreteria Amm.va	A) a)Archivio degli insediamenti produttivi; b)archivio ditte per gare d'appalto del Comune/LLPP e forniture; c)Richieste di accesso atti comunali;	A) a)Dati penali nella gestione delle gare d'appalto LLPP.

	d) Incarichi professionali; e)contratti lavori pubblici; f)richieste accesso atti.	
7 Commercio	A) a)Richieste di accesso atti comunali; b)archivio autorizzazioni al commercio fisso, pubblici esercizi, commercio su aree private; c)archivio autorizzazioni commercio su aree pubbliche, controllo pesi e misure; d)ordinanze.	A) a)Dati penali nell'ambito dei procedimenti relativi al rilascio e/o revoca di autorizzazioni commerciali; b)dati sensibili in relazione al rilascio di autorizzazione al commercio su area pubblica.
8 Urbanistica	A) a)ordinanze sindacali e dirigenziali; b)edilizia agevolata e convenzionata; c)edilizia sovvenzionata; d)certificazione destinazione urbanistica; e)pareri di massima in materia urbanistica; f)osservazioni agli strumenti urbanistici; g)piani particolareggiati; h)attestazioni varie in materia urbanistica; i)autorizzazioni vendita PEEP; j)collaudi opere di urbanizzazione e relativi piani particolareggiati; k)convenzioni urbanistiche; l)richieste variazioni PRG.	A) a)
9 Edilizia privata	A) a)archivio degli insediamenti produttivi; b)ordinanze sindacali e dirigenziali; c)concessioni edilizie; d)condono edilizio – abusi edilizi; e)banche dati ingiunzioni e diffide; f)verifica abitabilità per cittadini extracomunitari; g)autorizzazioni edilizie; h)denunce inizio attività; i)certificazioni destinazione urbanistica; j)ISTAT k)insegne pubblicitarie; l)ascensori; m)attività estrattive; n)cemento armato; o)perforazione pozzi; p)dati catastali; q)espropri;	A) a)Dati sensibili nella gestione del rilascio delle concessioni edilizie; b)dati sensibili nella gestione del rilascio delle autorizzazioni edilizie; c)dati sensibili nella gestione delle denunce inizio attività; d)dati sensibili nella gestione delle pratiche di condono edilizio; e)dati sensibili nella gestione delle ingiunzioni e diffide; f)dati sensibili nella gestione delle ordinanze sindacali e dirigenziali; g)dati sensibili nella gestione delle concessioni edilizie.

10 Progettazione	A) a)richieste accesso atti.	A) a)Dati penali nelle gare d'appalto LLPP e nella gestione dei contratti.
11 Manutenzione	A) a)Dati fornitori e relativi contratti; b)gestione dei dati immobiliari; c)dati catastali; d)richieste accesso dati.	A) a)Dati penali nella gestione delle gare d'appalto LLPP
12 Polizia Municipale	A) a)Verbali di contestazione alle violazioni del codice della strada; b)violazioni amm.ve di altro genere; c)cessioni e locazioni di fabbricati ex L. 191/78; d)controllo residenze; e)veicoli rubati e recuperati; f)gestione per rilascio contrassegno sose in deroga centro storico; g)incidenti stradali; h)anagrafe popolazione residente emigrata o deceduta; i)archivio verbali illeciti al NCS; j)presa visione documenti; k)registro porto d'armi; l)pagamento violazioni; m)Passi carrabili;	A) a)Dati sensibili trattati per le pratiche di incidenti stradali; b)dati sensibili per autorizzazioni per soste spazi invalidi; c)dati sensibili relativi a presa visione di documenti; d)dati sensibili per denunce infortuni sul lavoro; e)dati sensibili per autorizzazione per manifestazioni politiche o religiose; f)dati penali per incidenti stradali; g)dati penali per attività di polizia giudiziaria; h)dati penali per presa visione documenti.

CAPITOLO II

Analisi dei rischi e misure da adottare per garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali.

I possibili rischi individuati sono i seguenti:

AREE E LOCALI	• Intrusione • Ingresso non controllato o non autorizzato • Incendio
INTEGRITÀ E DISPONIBILITA' DEI DATI	• Danneggiamento, perdita, alterazione a causa di: o virus o mancanza di energia elettrica o avaria o accessi non consentiti o non autorizzati o furti o manomissioni hardware e software o allagamento o non conoscenza da parte degli incaricati delle procedure informatiche, delle misure di sicurezza, dei rischi • Danneggiamento, perdita, alterazione dei supporti di memorizzazione a causa di: o furti o copie abusive o incendio o allagamento • Danneggiamento, perdita, alterazione dei dati durante la trasmissione degli stessi a causa di: o intercettazione o errore di invio / mancata destinazione o avaria o intrusione di terzi non autorizzati o virus • Danneggiamento, perdita, alterazione dei dati su cartaceo.

La gravità del rischio viene calcolata tramite degli indici che individuano probabilità (indice P) e gravità del danno (D) di ogni possibile evento.
Il rischio quindi non è altro che la risultante della probabilità che un evento accada e del danno che questo comporta.

Secondo questi criteri, dando a P ed a D un valore da 1 a 4 si otterrà per R (rischio) un range di valori da 1 a 16.
L'indice R sarà quindi misura della classe di rischio.

Valori degli indici:

Probabilità: (P)	1	Improbabile
	2	Poco Probabile
	3	Probabile
	4	Altamente probabile
Danno (D)	1	Lieve
	2	Medio
	3	Grave
	4	Gravissimo

In relazione all'indice R si identifica quale misura dovrà essere adottata per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti al fine della loro custodia e accessibilità.

In considerazione del fatto che il rischio 0 assoluto non può esistere si determina il livello di sopportazione del rischio:

- Sopportazione da 1 a 4
- Riduzione del rischio oltre 4

AREE E LOCALI:

RISCHIO INTRUSIONE:

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- Durante le ore notturne le porte di accesso principale alla struttura vengono chiuse;
- Sono previsti vetri antisfondamento su tutte le aree degli uffici amministrativi;
- Esiste un sistema di antiintrusione con collegamento telefonico alle forze dell' ordine per quanto riguarda l' ufficio anagrafe.

Evento	Probabilità	Danno	Rischio
Intrusione	1	3	3

MISURE DA ADOTTARE:

- nessuna

RISCHIO DI INGRESSO non controllato o non autorizzato:

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- Gli accessi dei dipendenti vengono controllati tramite registrazione con badge magnetico;
- Le chiavi delle porte di accesso agli uffici amministrativi sono in possesso del personale amministrativo, del sindaco e amministratori;
- Il router e il nas sono posizionati in rack dotato di chiave in possesso degli amministratori, luogo comunque accessibile solo ai dipendenti ed altri eventuali soggetti autorizzati;
- Al di fuori delle aree di accesso consentite al pubblico, eventuali visitatori e/o prestatori di mano d' opera sono accompagnati e vigilati dal personale in servizio.

Evento	Probabilità	Danno	Rischio
Ingresso non controllato o non autorizzato	1	3	3

MISURE DA ADOTTARE:

- nessuna

RISCHIO DANNEGGIAMENTO per incendio:

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- All' interno della struttura sono presenti estintori a norma di legge.

Evento	Probabilità	Danno	Rischio
Incendio	1	4	4

MISURE DA ADOTTARE:

- nessuna

DATI

RISCHIO DANNEGGIAMENTO,PERDITA, ALTERAZIONE a causa di virus:

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- Sul Server e su tutti i Pc sono stati installati software antivirus il cui aggiornamento avviene giornalmente in modalità automaticamente da Internet;
- Un dispositivo firewall hardware limita l'accesso ad Internet solo i pc autorizzati e solo per determinati intervalli di tempo.

Evento	Probabilità	Danno	Rischio
Virus	1	4	4

MISURE DA ADOTTARE:

- nessuna

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE a causa di mancanza di energia elettrica:

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- L' impianto elettrico è a norma.
- E' stato installato un gruppo di continuità a protezione del Server e dei singoli PC. E' stato inoltre impostato lo spegnimento automatico del Server in caso di prolungata assenza di energia elettrica.

Evento	Probabilità	Danno	Rischio
Perdita dati (per mancanza energia elettrica)	1	2	2

MISURE DA ADOTTARE:

- nessuna

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE a causa di avaria del sistema informatico o dei software installati:

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- Esecuzione del back up di dati e programmi con cadenza settimanale su un supporto magnetico di capacità adeguata alle dimensioni degli archivi;
- Le cassette su cui viene effettuato il back up sono 3 e riportano l' indicazione del giorno;
- I supporti contenenti i dati del back - up sono conservate all' interno dell' ufficio ragioneria;
- L' eventuale perdita di dati viene ripristinata dai supporti contenenti back up;
- E' previsto un ulteriore backup su dispositivo Nas collocato in un rack dotato di chiave. Il backup avviene giornalmente;
- In casi particolari (protocollo), il back-up viene effettuato localmente nell'ambito di taluni uffici. In questo caso l'incaricato effettua le seguenti operazioni:
  - esecuzione quotidiana del backup, eventualmente attraverso procedure automatiche;
  - verifica periodica della corretta esecuzione del backup;
  - mantenimento di un elenco dei backup effettuati;
  - archiviazione dei supporti secondo le disposizioni precedentemente elencate;
  - effettivo ripristino dei dati in caso di necessità.
- E' stato stipulato un contratto di assistenza hardware e sistemistica con la Ditta Microweb di Villa Agnedo

Evento	Probabilità	Danno	Rischio
Perdita dati causa avaria	2	3	6

MISURE DA ADOTTARE:

- Prevedere inoltre una cassetta di back up periodica;
- Custodire i supporti contenenti i dati del back - up in cassaforte ignifuga.
- Prevedere il trasferimento di eventuali dati locali sul server.

RISCHIO DANNEGGIAMENTO per allagamento:

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- Il Server e i Pc presenti nell' Ente sono stati rialzati da terra e posti su idonei supporti;

Evento	Probabilità	Danno	Rischio
Allagamento	1	2	2

MISURE DA ADOTTARE:

- nessuna

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE a causa di accessi non consentiti o non autorizzati, furti o manomissioni hardware e software, non conoscenza da parte degli incaricati delle procedure informatiche, delle misure di sicurezza, dei rischi

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- L' accesso ai dati è consentito solo tramite inserimento di codice identificativo personale e parola chiave attribuiti ad ogni utente;
- Presso ciascun Ufficio è consentita l'installazione esclusiva delle seguenti tre categorie di software:
  - software commerciale, dotato di licenza d'uso;
  - software gestionale realizzato specificatamente per l'amministrazione comunale dalle ditte specializzate nel settore della pubblica amministrazione;
  - software realizzato internamente per soddisfare eventuali esigenze particolari del singolo servizio.
- L'eventuale installazione di software diversi da quelli citati al punto precedente deve essere preventivamente valutata ed autorizzata dall' amministratore del sistema;
- Al fine di prevenire ed evitare la diffusione di virus informatici, il software viene installato solo da supporti fisici originali, dei quali è ben nota la provenienza. In mancanza di procedure di installazione automatiche, il responsabile del trattamento è stato istruito per effettuare l'aggiornamento del software antivirus sulle postazioni di lavoro di sua competenza, con cadenza settimanale;
- Gli incaricati sono stati istruiti per il corretto utilizzo dei Pc e del sistema informatico presente nell' Ente.

Evento	Probabilità	Danno	Rischio
Accesso non consentito ai dati	1	3	3
Manomissione hardware / software	1	3	3
Furto	1	4	4
Ignoranza delle procedure informatiche, delle misure di sicurezza e dei rischi	4	3	12

MISURE DA ADOTTARE:

- Prevedere per quanto riguarda l'accesso ad Internet e alla posta elettronica, la sicurezza di un ulteriore software antivirus installato sul mail server;
- Prevedere formazione agli incaricati in merito alle misure di sicurezza adottate ed in particolare del documento programmatico sulla sicurezza.

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE dei dati su supporti di memorizzazione a causa di furti, copie abusive, incendio, allagamento, danneggiamento o alterazione dei supporti

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- I supporti di back up vengono rinnovati con periodicità annuale;

Evento	Probabilità	Danno	Rischio
Furto	1	2	2
Copia abusiva	1	3	3
Incendio	1	3	3
Allagamento	1	2	2

MISURE DA ADOTTARE:

- Prevedere che un supporto di back up venga custodito all'esterno dell' Ente e venga aggiornato settimanalmente;
- Prevedere di fornire istruzioni ed indicazioni agli incaricati relativamente al riutilizzo di supporti informatici (floppy e cd rom) contenenti dati sensibili.

RISCHIO DANNEGGIAMENTO, PERDITA, ALTERAZIONE DI DATI DURANTE L'INVIO DEGLI STESSI per intercettazione, errore di invio, mancata destinazione, avaria, intrusione di terzi non autorizzati, virus.

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- Le trasmissioni sono protette da antivirus aggiornato giornalmente in automatico da Internet;
- E' stato fatto divieto di utilizzare le trasmissioni per l' invio di dati sensibili.
- L'accesso remoto alla rete è consentito solo alla Ditta Informatica Trentina tramite l'inserimento di credenziali di autenticazione;

Evento	Probabilità	Danno	Rischio
Intercettazione	2	3	6
Errore di invio / mancata destinazione	2	3	6
Avaria	1	3	3
Intrusione di terzi non autorizzati	1	4	4

MISURE DA ADOTTARE:

- Prevedere l' attivazione della ricevuta di ritorno in fase di invio di posta elettronica;
- Consentire solo al agli incaricati il collegamento ad Internet tramite inserimento di credenziali di autenticazione;

RISCHIO DANNEGGIAMENTO, PERDITA DATI SU CARTACEO

MISURE DI SICUREZZA ATTUALMENTE ADOTTATE:

- Tutta la documentazione contenente dati personali sensibili è custodita in armadi dotati di serratura rialzati dal pavimento. La chiave di tali armadi è a disposizione solo dell'incaricato che ne cura la chiusura dopo l'utilizzo – limitando tali operazioni a quelle strettamente necessarie allo svolgimento dei compiti di ufficio – affinché nessun estraneo all'ufficio possa accedervi;
- In nessun caso viene fatta fotocopia dei documenti che contengono dati sensibili o penali a terze persone.

Evento	Probabilità	Danno	Rischio
Perdita dati cartaceo	1	2	2

MISURE DA ADOTTARE:

- nessuna

CAPITOLO III

CRITERI DI RIPRISTINO DATI E RELATIVE MODALITA'

(Punto 19.5 e 23 del disciplinare tecnico - all.B D.Lvo. 196/2003)

Responsabile interno di procedura: Samonati Ezio Battista

Il Responsabile della procedura di ripristino dati avrà il compito di coordinare le operazioni di recupero sotto riportate e di mantenere i rapporti con i soggetti / aziende esterne, incaricati del recupero stesso.

MISURE PREVENTIVE:

- Assicurarsi dell' effettiva esecuzione di Back up di sistema su server tramite consultazione del file di Log;
- Archiviare 1 copia di back up di sistema (PROGRAMMI E DATI) in luogo esterno alla sede operativa e aggiornarlo con cadenza non superiore ai sette giorni;
- Adottare specifici programmi di back up;
- Adottare specifici programmi di disaster recovery;
- Informare tempestivamente l'amministratore del sistema ed i responsabili del trattamento dati di ogni eventuale problema di sicurezza di cui dovesse venire a conoscenza;
- Informare tempestivamente gli incaricati e l'amministratore di sistema in presenza di virus negli elaboratori dell'ufficio, della prassi da parte del personale non conformi alle disposizioni di sicurezza, della periodica necessità di variazione delle parole chiave da parte degli incaricati e della disponibilità di programmi di aggiornamento relativi all'antivirus;
- Informare gli incaricati al fine di provvedere ad organizzare iniziative per l'illustrazione e la diffusione degli accorgimenti da adottare in tema di sicurezza;
- Verificare con il titolare ed eventualmente attivare la possibilità di un ulteriore back up effettuato da azienda esterna all'ente tramite hosting;
- Mantenere un elenco aggiornato di aziende in grado di fornire entro 5 gg dall' evento componenti hardware (server o personal computer) e assistenza sistemistica e software.

MISURE DI RIPRISTINO IN CASO DI PERDITA DI DATI E/O STRUMENTI ELETTRONICI:

- Contattare la il fornitore di componenti hardware e richiedere la fornitura entro 5 giorni della macchina server e delle ulteriori macchine danneggiate.
- Contattare il fornitore di servizi di assistenza sistemistica e concordare l' intervento per il ripristino di dati da Back up; (se non presente figura idonea alla mansione)
- Contattare il fornitore di eventuali ulteriori software per l' installazione ed il ripristino dei dati contenuti negli applicativi.
- In collaborazione con i vari responsabili di settore / servizi effettuare un controllo sui dati di competenza, al fine di verificare l' effettivo avvenuto ripristino dei dati stessi.

CAPITOLO IV

PIANO DI FORMAZIONE AGLI INCARICATI DEL TRATTAMENTO

Argomenti oggetto della formazione:

- Rischi
- Misure di Prevenzione
- Profili normativi in relazione alle mansioni
- Responsabilità che ne derivano
- Modalità di aggiornamento delle misure di sicurezza

Frequenza:

- Entrata in servizio;
- Cambiamento di mansioni;
- Introduzione di nuovi strumenti rilevanti rispetto al trattamento di dati personali.

Modalità di formazione:

- formazione tramite linee guida:
  - Redazione e consegna di guida formativa, mirata in base alle mansioni assegnate ai singoli incaricati;
  - Consegna di copia del documento programmatico sulla sicurezza.
  -
- formazione tramite corso:
  - docente esterno

Controllo: Verrà tenuto un calendario aggiornato dei partecipanti ai piani formativi.

CAPITOLO V

TRATTAMENTI ESTERNI:

criteri da adottare per garantire l'adozione delle misure minime di sicurezza

Nel contratto che prevede l' esercizio delle attività o nella nomina del responsabile, il soggetto esterno deve dichiarare di adottare le misure minime di sicurezza così come previsto dal disciplinare tecnico allegato al Codice.

Nel contratto che prevede l'esercizio delle attività o nella nomina a responsabile deve essere contemplata la possibilità da parte del titolare del trattamento di effettuare verifiche sui trattamenti svolti per conto della società dal soggetto esterno.

In seguito alla nomina a responsabile o alla delega dell' attività, a seconda della tipologia di incarico e delle operazioni affidate allo stesso, il controllo delle misure di sicurezza deve avvenire verificandone l'esistenza tramite elaborazione di una check-list redatta dal titolare e da compilarsi a cura del soggetto esterno, la cui traccia può essere la seguente:

- Richiesta dei soggetti incaricati, preposti al trattamenti dei dati personali affidati alla struttura esterna;
- Richiesta di copia del documento programmatico sulla sicurezza;
- Richiesta di copia della licenza di acquisto di antivirus.
- Copia delle istruzioni impartite agli incaricati;
- Programma della formazione agli incaricati;
- Tipo di sistema antintrusione installato (marca e modello);
- Periodicità e luogo di custodia del Back – up;
- Certificazione di installazione delle misure minime in conformità al disciplinare tecnico (se installate da soggetti esterni);

Di regola rimane comunque vietato il trasferimento di dati sensibili tramite internet; la comunicazione è consentita solo previa autorizzazione del responsabile del trattamento.

CAPITOLO VI

Periodicità e modalità dei controlli

Il responsabile dei controlli sulle misure di sicurezza informatiche avrà il compito di provvedere, personalmente o tramite aziende specializzate, alla verifica della funzionalità e dell' efficienza delle misure di sicurezza adottate.
Dovrà essere redatto l' apposito verbale con gli esiti delle verifiche stesse la cui traccia è indicata nello schema di cui all' allegato A.

Responsabile dei controlli: responsabile del trattamento dei dati interno

Cadenza dei controlli: sei mesi

COMUNE DI BIENO

Allegato A :Verbale di controllo informatico sulle misure di sicurezza

Titolare del Trattamento: COMUNE DI BIENO

Misure di sicurezza	Descrizione	note
Credenziali di autenticazione	☑ Codice identificativo personale + password ☐ Dispositivo di autenticazione ☐ Caratteristiche biomediche	☑ Non si rilevano problemi ☐ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Profili di autorizzazione	Assegnati a n° 10 incaricati	☑ Non si rilevano problemi ☐ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Antivirus	Modalità: ☑ Automatica ☐ Manuale Ultima data aggiornamento: 01 / 01 / 2008	☑ Non si rilevano problemi ☐ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Aggiornamenti periodici dei programmi (patch)	Programma MAGGIOL Aggiornato il 02 / 02 / 2008 Programma _____ Aggiornato il ___/___/_____	☑ Non si rilevano problemi ☐ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Back up	Modalità: ☑ Automatica ☐ Manuale Data inizio utilizzo supporto: 01 / 01 / 2008	☑ Non si rilevano problemi ☐ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Gruppo di continuità	☑ Sui Pc ☑ Sul server	☑ Non si rilevano problemi ☐ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____

COMUNE DI BIENO

Raid	Tipologia □ Hardware □ Software □ Raid 1 □ Raid 5 □ Altro	□ Non si rilevano problemi □ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Modem	Sconnessione □ Automatica □ Manuale	□ Non si rilevano problemi □ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Router	Sconnessione ☑ Automatica □ Manuale	☑ Non si rilevano problemi □ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Firewall	☑ Hardware □ Software	☑ Non si rilevano problemi □ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Accesso remoto alla rete	Modalità □ Linea diretta □ Internet ☑ Autenticazione PWD ed ID □ Controllo numero chiamante □ Richiamata	☑ Non si rilevano problemi □ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Trattamento disgiunto dei dati sensibili da altri dati	Modalità □ Crittografia □ Codifica Disabilitazione del campo in base al profilo	□ Non si rilevano problemi □ Si rilevano problemi dovuti a: ▪ _____ ▪ _____ ▪ _____ Consigli: _____
Altro (indicare)		

Data del controllo

26/03/2008

Firma

Allegato B

RESPONSABILI IN RELAZIONE AL TRATTAMENTO DEI DATI:

Titolare del Trattamento: COMUNE DI BIENO

Responsabile dell' Ufficio: Menguzzo Stefano

Responsabile del Trattamento interni: Menguzzo Stefano

Responsabili del Trattamento esterni:

- **I.T. di Trento per la Gestione paghe e contributi**
- **Informatica Trentina per la Contabilità Generale e trasmissione dati richiesti dalla Provincia Autonoma di Trento**
- **Cba di Rovereto**
- **Ditta Emmetre per programma Maggioli anagrafe**
- **Il Comprensorio C3 per quanto riguarda i dati relativi alla gestione della Tariffa rifiuti RSU**
- **Il Medico Competente ai sensi della legge 626 per quanto riguarda la sicurezza sui luoghi di lavoro**
- **Il Consulente del Consorzio Lavoro Ambiente responsabile della Sicurezza sul luogo di lavoro**
- **Il Revisore dei Conti per quanto riguarda la documentazione del Comune**
- **La Tesoreria Comunale**
- **Riscossione Uno Spa**
- **Emmetre per la Gestione anagrafe, stato civile ed elettorale**

Responsabili dei diritti dell'interessato: Menguzzo Stefano

Custode delle password: Samonati Ezio Battista

Incaricati:

- **Segreteria generale : Stefano Menguzzo**
- **Personale e organizzazione : Nicoletta Capra**
- **Archivio e protocollo : Samonati Ezio Battista**
- **Servizi demografico/elettorali : Marietti Maria Giuseppina**
- **Tributi : Nicoletta Capra e per ICI Samonati Ezio Battista**
- **Segreteria amministrativa : Stefano Menguzzo**
- **Commercio : Marietti Maria Giuseppina**
- **Urbanistica : Luigi Ferrai**
- **Edilizia privata : Luigi Ferrai**
- **Progettazione : Luigi Ferrai**
- **Polizia Municipale: Vigile incaricato dal Corpo di Polizia Locale intercomunale**
- **Manutenzione : Luigi Ferrai**

Per ogni categoria di soggetti sopra esposti verrà allegato al presente documento copia della nomina contenente i compiti e le responsabilità in relazione al trattamento di dati.