I.E.G

IMMEDIATA ESECUTIVITÀ

La presente deliberazione viene affissa il 4 APR. 2006 *all'Albo Pretorio per rimanervi 15 giorni*

PROVINCIA di BENEVENTO

Deliberazione della Giunta Provinciale di Benevento n. 182 ***del*** 31 MAR. 2006

OGGETTO: ***Approvazione del "Documento Programmatico sulla Sicurezza" (DPS) ai sensi dell'art. 34 – comma 1, lett. g) e della Regola 19 dell'Allegato B del Codice in materia di protezione di dati personali (D. Lgs 30 giugno 2003 n. 196).***

L'anno duemilasei il giorno trentuno del mese di Marzo presso la Rocca dei Rettori si è riunita la Giunta Provinciale con l'intervento dei Signori:

1) On.le Carmine NARDONE	- Presidente	
2) Dr. Pietro GIACCONARDO	- ~~Vice Presidente~~ Assessore	
3) Rag. Alfonso CIERVO	- Assessore	
4) Ing. Pompilio FORGIONE	- Assessore	ASSENTE
5) Dott. Pasquale GRIMALDI	- Assessore	
6) Dott. Giorgio Carlo NISTA	- Assessore	
7) Dott. Carlo PETRIELLA	- Assessore	
8) Dott. Rosario SPATAFORA	- Assessore	ASSENTE
9) Geom. Carmine VALENTINO	- Assessore	

Con la partecipazione del Segretario Generale Dott. Gianclaudio IANNELLA

L'ASSESSORE PROPONENTE: dott. Pasquale GRIMALDI -

LA GIUNTA

PREMESSO che con delibera di Consiglio Provinciale n. 97 del 21.12.2005 è stato approvato il Regolamento per il trattamento dei dati sensibili e giudiziari della Provincia di Benevento, ai sensi del D. Lgs. n. 196/2003;

VISTO il D. Lgs 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali*" (d'ora innanzi Codice);

VISTO, in particolare, l'art. 34 – comma 1, lett. g) – e la Regola 19 dell'Allegato B al Codice i quali prescrivono che il titolare di trattamenti di dati sensibili e/o di dati giudiziari debba redigere un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

CONSIDERATO che in data 13 maggio 2004 l'"*Ufficio del Garante per la protezione dei dati personali*" ha pubblicato un documento intitolato <<*Prime riflessioni sui criteri di redazione del Documento Programmatico sulla Sicurezza*>>;

VISTO il "*Documento Programmatico sulla Sicurezza*" allegato alla presente deliberazione della quale costituisce parte integrante e sostanziale e dato atto che lo stesso è stato predisposto dalla società CM CONSIT S.p.A., incaricata con determina dirigenziale n. 2026/02 del 18.10.2005, tenendo conto delle indicazioni fornite dal "*Garante per la protezione dei dati personali*" nel documento sopra citato e ritenuto di approvarlo;

DATO ATTO che tale documento è stato trasmesso ai Dirigenti dell'Amministrazione Provinciale con nota n. 1319/SEP del 15.02.2006;

DATO ATTO, altresì, che nessuna richiesta di modifica e/o integrazione, né alcun rilievo sono pervenuti da parte dei Dirigenti dell'Ente;

RITENUTO di disporre che tutte le strutture dell'Ente siano tenute ad adeguarsi alle prescrizioni contenute nel presente "DPS";

DATO ATTO che, ai sensi dell'art. 180 - comma 1 (*così come modificato dalla legge n. 51 del 23 febbraio 2006 di conversione in legge, con modificazioni, del decreto-legge 30 dicembre 2005, n. 273*), e della regola 19 dell'Allegato B al Codice, il "*Documento Programmatico sulla Sicurezza*" deve essere adottato entro il 31 marzo 2006 ed aggiornato successivamente entro il 31 marzo di ogni anno;

DATO ATTO, inoltre, che ai sensi della Regola 26 dell'Allegato B al Codice e del parere espresso dal "Garante per la protezione dei dati personali" in data 22 marzo 2004 è necessario fare riferimento, nella relazione di accompagnamento a ciascun Bilancio di Previsione, circa l'avvenuta redazione o aggiornamento del DPS;

Esprime parere favorevole circa la regolarità tecnica della proposta.

Lì_____

Il DIRIGENTE del SETTORE
EDILIZIA e PATRIMONIO
ing. Valentino Melillo

Esprime parere favorevole circa la regolarità contabile della proposta

Lì_____

IL DIRIGENTE del Settore FINANZE
E CONTROLLO ECONOMICO
dott. Sergio MUOLLO

LA GIUNTA

Su relazione dell'Assessore al ramo, dott. Pasquale GRIMALDI;

A voti unanimi

DELIBERA

Per i motivi espressi in narrativa e che formano parte integrante e sostanziale del presente dispositivo:

- **di approvare** il "***Documento Programmatico sulla Sicurezza***" (DPS) allegato (sub lettera A) alla presente deliberazione e costituente parte integrante della stessa;

- **di disporre** che tutte le Strutture dell'Ente siano tenute ad adeguarsi alle prescrizione contenute nell'allegato "DPS";

- **di dare atto** che – ai sensi dell'art. 180, comma 1 (*così come modificato dalla legge n. 51 del 23 febbraio 2006 di conversione in legge, con modificazioni, del decreto-legge 30 dicembre 2005, n. 273*), e della regola 19 dell'Allegato B al Codice (D. Lgs n. 196/2003) il "*Documento Programmatico sulla Sicurezza*" deve essere aggiornato successivamente, entro il 31 marzo di ogni anno;

- **di disporre** ai sensi della Regola 26 dell'Allegato B al Codice e del parere espresso dal "Garante per la protezione dei dati personali" in data 22 marzo 2004 è necessario fare riferimento, nella relazione di accompagnamento a ciascun Bilancio di Previsione, circa l'avvenuta redazione o aggiornamento del DPS;

- **di dichiarare** la presente deliberazione immediatamente esecutiva.

VISTO l'art. 180 - commi 1, 2 e 3, del Codice il quale prevede che:

1. Le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, sono adottate entro il 31 marzo 2006.

2. Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura.

3. Nel caso di cui al comma 2, il titolare adotta ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31, adeguando i medesimi strumenti al più tardi entro il 30 giugno 2006;

DATO ATTO che la presente deliberazione non comporta assunzioni di spesa e pertanto non è "rilevante ai fini contabili";

Per tutte le motivazioni sopra esposte si

PROPONE:

- di approvare il "*Documento Programmatico sulla Sicurezza*" (DPS) allegato (sub lettera A) alla presente deliberazione e costituente parte integrante della stessa;

- di disporre che tutte le Strutture dell'Ente siano tenute ad adeguarsi alle prescrizione contenute nell'allegato "DPS";

- di dare atto che - ai sensi dell'art. 180, comma 1 (*così come modificato dalla legge n. 51 del 23 febbraio 2006 di conversione in legge, con modificazioni, del decreto-legge 30 dicembre 2005, n. 273*), e della regola 19 dell'Allegato B al Codice (D. Lgs n. 196/2003) il "*Documento Programmatico sulla Sicurezza*", deve essere aggiornato successivamente entro il 31 marzo di ogni anno;

- di disporre ai sensi della Regola 26 dell'Allegato B al Codice e del parere espresso dal "Garante per la protezione dei dati personali" in data 22 marzo 2004 è necessario fare riferimento, nella relazione di accompagnamento a ciascun Bilancio di Previsione, circa l'avvenuta redazione o aggiornamento del DPS;

Verbale letto, confermato e sottoscritto

IL SEGRETARIO GENERALE
(Dr. Gianclaudio IANNELLA)

IL PRESIDENTE
(On. Carmine NARDONE)

==========

N. 246 **Registro Pubblicazione**

Si certifica che la presente deliberazione è stata affissa all'Albo in data odierna, per rimanervi per 15 giorni consecutivi a norma dell'art. 124 del T.U. – D. Lgs.vo 18.8.2000, n.267.

BENEVENTO – 4 APR. 2006

IL MESSO

IL SEGRETARIO GENERALE
IL SEGRETARIO GENERALE
(Dott. Gianclaudio IANNELLA)

==========

La su estesa deliberazione è stata affissa all'Albo Pretorio in data – 4 APR. 2006 **e contestualmente comunicata ai Capigruppo ai sensi dell'art.125 del T.U. – D. Lgs.vo 18.8.2000, n.267.**

SI ATTESTA, che la presente deliberazione è divenuta esecutiva a norma dell'art. 124 dell'art.124 del T.U. – D Lgs.vo 18.8.2000, n.267.

lì 20 APR. 2006

IL RESPONSABILE DELL'UFFICIO

IL SEGRETARIO GENERALE
IL SEGRETARIO GENERALE
F.to Dott. Gianclaudio IANNELLA

==========

Si certifica che la presente deliberazione è divenuta esecutiva ai sensi del T.U. – D Lgs.vo 18.8.2000, n. 267 il giorno 20 APR. 2006

☒ Dichiarata immediatamente eseguibile (Art. 134, comma 4, D. Lgs.vo 18.8.2000, n. 267)

☐ Decorsi 10 giorni dalla sua pubblicazione (Art. 134, comma 3, D. Lgs.vo 18.8.2000, n. 267).

☐ E' stata revocata con atto n. _____ del _____

Benevento lì 20 APR. 2006

Il SEGRETARIO GENERALE
IL SEGRETARIO GENERALE
Dott. Gianclaudio IANNELLA

==========

Copia per:

SETTORE Tutti a mezzo PEC il _____ prot. n. Es 3162 24.4.06

SETTORE Servizi ai cittadini il 2751 prot. n. _____

SETTORE _____ il 2756 6.4.06 prot. n. _____

Revisori dei Conti il 6.4.06 prot. n. _____

X Nucleo di Valutazione il _____ prot. n. _____

Conferenza Capigruppo

513
4-4-06

PROVINCIA di BENEVENTO

Settore Servizi ai Cittadini

Servizio Affari Generali

Prot. n. 9151

Benevento, lì 6 APR. 2006

U.O.: GIUNTA/CONSIGLIO

AL **DIRIGENTE DEL SETTORE PATRIMONIO**

AI **SIGG.RI DIRIGENTI:**

Dr.	Sergio MUOLLO
Ing.	Angelo FUSCHINI
Dr.ssa	Alfonsina COLARUSSO
Dr.	Luigi VELLECA
Dr.ssa	Elisabetta CUOCO
Avv.	Vincenzo CATALANO
Dr.ssa	Giovanna ROMANO
Ing.	Angelo D'ANGELO
Dr.	Ludovico BARONE

AL **PRESIDENTE NUCLEO DI VALUTAZIONE**
SEDE

Oggetto: **Delibera G.P. N. 182 del 31.3.2006 ad oggetto: "Approvazione del "Documento Programmatico sulla Sicurezza" (DPS) ai sensi dell'art. 34 – comma 1, lett. g) e della Regola 19 dell'Allegato B del Codice in materia di protezione di dati personali (D. Lgs 30 giugno 2003 n. 196)" -**

Per quanto di competenza, si rimette copia della delibera indicata in oggetto, immediatamente esecutiva.

IL DIRIGENTE DEL SETTORE
- Dr. ssa Patrizia TARANTO -

1. INTRODUZIONE

1.1. PREMESSA

L'attività resa necessaria dalle disposizioni previste nel nuovo "Codice per la Protezione dei dati Personali" (di seguito Testo Unico), ha portato la Provincia di Benevento ad effettuare un'analisi approfondita delle proprie necessità organizzative, fisiche e logiche di gestione dei dati personali.

I risultati del lavoro svolto sono illustrati nel presente documento che prende in esame sia le misure che il legislatore ha prescritto obbligatoriamente in quanto necessarie e sufficienti ad escludere i rischi particolarmente gravi per i dati sottoposti a trattamento (misure minime), sia le c.d. misure idonee, rivolte a ridurre al minimo i rischi di distruzione o di perdita anche accidentale dei dati, di accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

In particolare, coerentemente con il "Disciplinare Tecnico in materia di misure minime di sicurezza" che ha sostituito, dal 1° gennaio 2004, il DPR 318/99, saranno illustrate le misure di sicurezza organizzative, fisiche e tecnologiche che la Provincia di Benevento ha predisposto, o si sta accingendo a predisporre entro i termini di legge, in modo da ridurre al minimo i rischi derivanti dal trattamento dei dati personali.

1.2. FINALITÀ DEL DOCUMENTO

In relazione alle attività di adeguamento di cui sopra, il presente documento persegue l'obiettivo di:

- chiarire sotto il nuovo profilo normativo gli obblighi che l' Ente deve adempiere in merito all'adozione delle misure di sicurezza;
- tutelare gli interessi dei soggetti pubblici e privati che fanno affidamento sui trattamenti svolti dall' Ente;
- evitare eventi pregiudizievoli che possano danneggiare disponibilità, riservatezza e integrità del patrimonio di dati dell' Ente;
- potenziare la consapevolezza dei rischi e delle insidie che possono coinvolgere la gestione e l'utilizzo dei sistemi informativi automatizzati e degli archivi cartacei;
- indicare possibili soluzioni tecnico/organizzative per prevenire situazioni di pericolo per le risorse e per chi se ne avvale, nonché per affrontare e risolvere eventuali problemi derivanti dal verificarsi di eventi lesivi del patrimonio informativo;
- individuare le misure di sicurezza già adottate o da implementarsi in modo da ridurre al minimo i rischi:
    - di distruzione o perdita, anche accidentale dei dati;
    - di accesso non autorizzato;
    - di trattamento non consentito o non conforme alla finalità della raccolta dei dati.

1.3. STRUTTURA DEL DOCUMENTO

Il presente documento è articolato nelle seguenti sezioni:

INDICE DEI CONTENUTI

PROVINCIA DI BENEVENTO	DOCUMENTAZIONE PRIVACY	
	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Revisione **2.0** Data **20/12/2005** Pagina **1** di **54**
Documento redatto da: CM Consit S.p.A.	**Documento verificato da:**	**Documento approvato da:**

- elenco dei trattamenti di dati personali: contiene lo stato dell'arte dell' Ente in termini di trattamenti svolti;
- distribuzione dei compiti e delle responsabilità: riporta la distribuzione delle responsabilità all'interno e all'esterno della Provincia di Benevento, coerentemente con quanto prescritto nel Testo Unico;
- misure di sicurezza adottate: contiene l'elenco delle misure di sicurezza (misure minime e misure idonee) adottate alla data di stesura del presente documento;
- analisi dei rischi che incombono sui dati: contiene l'analisi dei rischi in relazione alle misure di sicurezza adottate;
- criteri e modalità per il ripristino della disponibilità dei dati sensibili o giudiziari: contiene le procedure adottate per garantire il ripristino dei suddetti dati in caso di distruzione o danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;
- elaborazione di un piano di formazione: contiene il piano di formazione previsto per sensibilizzare il personale sui temi e le problematiche applicative legate alla normativa sulla Privacy;
- criteri per garantire l'adozione delle misure di sicurezza in caso di trattamenti affidati all'esterno della struttura: contiene i criteri utilizzati dalla Provincia di Benevento per garantire che i dati personali affidati in gestione ai Responsabili esterni siano correttamente protetti con le misure di sicurezza previste dal dettato normativo;

1.4. AMBITO DI APPLICAZIONE

Il presente documento ha validità all'interno della Provincia di Benevento, con sede legale in Benevento, Piazza Castello – Rocca dei Rettori, operante attraverso le seguenti sede operative:

- Largo Carducci
- Via 25 Luglio
- Via Clino Ricci
- Via Santa Colomba
- Via Martiri d'Ungheria
- Corso Garibaldi
- Rocca dei Rettori
- Museo del Sannio
- Villa dei Papi
- Centri per l'impiego periferici

Il documento fa riferimento a tutti i trattamenti effettuati dalla Provincia di Benevento, con qualsiasi modalità, sia informatica sia cartacea, concernenti ogni tipologia di dato sia comune sia sensibile/giudiziario.

2. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Di seguito sono elencati i trattamenti dei dati personali svolti dalla Provincia di Benevento:

TRATTAMENTO	CATEGORIA DI INTERESSATI	NATURA DEI DATI TRATTATI			STRUTTURA DI RIFERIMENTO	ALTRE STRUTTURE ESTERNE CHE CONCORRONO AL TRATTAMENTO (ANCHE COMUNICAZIONE)
		Comuni	Sensibili	Giudiziari		
Formazione Professionale (Controllo sulle scuole di formazione professionale)	Titolari Scuole formazione professionale, Insegnati, Allievi	X		X	Politiche del Lavoro	Regione Campania (Assessorato del lavoro), aziende, ASL, INPS, INAIL, Enti Pubblici, Polizia Giudiziaria, Agenzia Entrate
Collocamento obbligatorio (disabili) - Verbale di accertamento sanitario	Candidati	X	X		Politiche del Lavoro	
Collocamento Ordinario	Enti, aziende, titolari aziende, candidati	X	X		Politiche del Lavoro	
Edilizia Scolastica	Persone Fisiche e Giuridiche	X		X	Edilizia e Patrimonio	
Edilizia Pubblica	Persone Fisiche e Giuridiche	X		X	Edilizia e Patrimonio	
Gestione Autoparco	Persone Fisiche e Giuridiche	X		X	Edilizia e Patrimonio	
Espropriazioni e Cartografia	Persone Fisiche	X			Edilizia e Patrimonio	Banche per la liquidazione dei proprietari espropriati
Pagamento incidenti stradali	Persone Fisiche	X			Edilizia e Patrimonio	
Occupazione Terreni	Proprietari terrieri	X			Agricoltura - Politiche Territorio Rurale e Forestale	
Autorizzazione Tagli Boschivi	Proprietari terrieri persone fisiche, persone giuridiche, enti territoriali	X			Agricoltura - Politiche Territorio Rurale e Forestale	Regione Campania
Vincolo Idrogeologico (trasferimenti/mutamenti terreni vincolati)	Proprietari terrieri persone fisiche, persone giuridiche, enti territoriali	X			Agricoltura - Politiche Territorio Rurale e Forestale	Regione Campania

Forestazione	operai/idraulici forestali	X			Agricoltura - Politiche Territorio Rurale e Forestale	
Amministrazione Forestazione	operai/idraulici forestali, familiari				Agricoltura - Politiche Territorio Rurale e Forestale	Regione, Banca Popolare di Novara, INAIL, INPS
Pesca (licenze di pesca sportiva)	Persone Fisiche	X			Agricoltura - Politiche Territorio Rurale e Forestale	Regione
Forniture di ripopolamento ittico	Persone Giuridiche	X			Agricoltura - Politiche Territorio Rurale e Forestale	ASL
Caccia - Esami di abilitazione venatoria	Cacciatori	X	X		Agricoltura - Politiche Territorio Rurale e Forestale	
Caccia - Ambito territoriale di caccia	Cacciatori	X			Agricoltura - Politiche Territorio Rurale e Forestale	ATC Regione
Caccia - Rilascio Tesserino Regionale Venatorio	Persone Fisiche	X			Agricoltura - Politiche Territorio Rurale e Forestale	Regione, Comuni
Detenzione Fauna per allevamento amatoriale	Persone Fisiche	X			Agricoltura - Politiche Territorio Rurale e Forestale	
Forniture di ripopolamento Faunistico	Persone Giuridiche	X			Agricoltura - Politiche Territorio Rurale e Forestale	ASL
Caccia al Cinghiale	Cacciatori	X			Agricoltura - Politiche Territorio Rurale e Forestale	Comuni, Polizia Provinciale, Corpo Forestale
POR - 1 Istanza di Finanziamento (Atti progettuali a amministrativi)	Persone fisiche e Giuridiche, Enti Pubblici, Comuni	X		X	Agricoltura - Interventi Strutturali e Sicurezza Alimentare	Regione Campania
Indennità su calamità naturali	Privati, Comuni	X		X	Agricoltura - Interventi Strutturali e Sicurezza Alimentare	

PSR - 1 di competenza	Persone fisiche e giuridiche	X		X	Agricoltura - Interventi Strutturali e Sicurezza Alimentare	Regione Campania
PSR - 2 di competenza	Persone fisiche e giuridiche	X		X	Agricoltura - Servizio Politiche Comunitarie e Agev. Fisc.	Regione Campania
POR - 2 Istanza di Finanziamento (Atti progettuali e amministrativi)	Persone fisiche e Giuridiche, Enti Pubblici, Comuni	X		X	Agricoltura - Servizio Politiche Comunitarie e Agev. Fisc.	Regione Campania
UMA (Agevolazioni Fiscali su Gasolio Agricolo)	Aziende Agricole, Persone Fisiche e Giuridiche	X			Agricoltura - Servizio Politiche Comunitarie e Agev. Fisc.	Guardia di Finanza, Agenzia Dogane
Organi Istituzionali		X	X	X	Servizi ai Cittadini	
Affari Generali		X	X	X	Servizi ai Cittadini	
Politiche Sociali - Assistenza Volontariato	Cittadini	X	X	X	Servizi ai Cittadini	Comune, Servizi Sociali, Vigili Urbani
Politiche Formative - Rapporti Università	Cittadini	X			Servizi ai Cittadini	
Promozione Sanitaria	Cittadini	X			Servizi ai Cittadini	
Turismo e Cultura	Associazioni, Cittadini	X			Servizi ai Cittadini	
Sport, Sviluppo economico e SUAP	Associazioni, Cittadini	X			Servizi ai Cittadini	
Previdenza	Associazioni, Cittadini	X	X	X	Servizi ai Cittadini	
Abusi Ambientali	Cittadini	X			Servizi ai Cittadini - Polizia Provinciale	Forze di Polizia/Autorità Giudiziaria
Polizia Mineraria	Cittadini	X			Servizi ai Cittadini - Polizia Provinciale	
Discarichi acque reflue	Cittadini	X			Servizi ai Cittadini - Polizia Provinciale	
Polizia stradale	Cittadini	X			Servizi ai Cittadini - Polizia Provinciale	
Faldone Personale	Dipendenti, Familiari, Parenti e Affini	X	X	X	Risorse Umane	Commissione Medica di Verifica, Società di Formazione
Retribuzioni	Dipendenti, Familiari	X	X	X	Risorse Umane	INPDAP, INPS, FILCOP, ENPAIA

Controllo Presenze - Ispezioni	Dipendenti, Familiari, Parenti e Affini	X	X	X	Risorse Umane	ASL (per visita fiscale), INAIL, Questura, Commissione Medica di Verifica, Comitato di Verifica delle Cause di Servizio (Roma)
Certificati Medici visite ex lg. 104	Dipendenti, Familiari	X	X		Risorse Umane	
Trasporto Persone - Gestione Fornitori	Persone fisiche e giuridiche	X		X	Mobilità ed Energia	Commissione Consultiva di Valutazione
Trasporto Merci c/proprio	Persone fisiche e giuridiche	X		X	Mobilità ed Energia	Commissione Consultiva di Valutazione
Trasporto Merci c/terzi	Persone fisiche e giuridiche	X		X	Mobilità ed Energia	Commissione Consultiva di Valutazione
Centri di Revisione	Persone fisiche e giuridiche	X		X	Mobilità ed Energia	
Studi di consulenza pratiche auto	Persone fisiche e giuridiche	X		X	Mobilità ed Energia	
Autoscuole	Persone fisiche e giuridiche	X		X	Mobilità ed Energia	
Contenzioso Civile/Lavoro	Dipendenti, Cittadini, Residenti, Persone Fisiche e Giuridiche	X	x	X	Avvocatura	Studi legali esterni, ex lg. 241/90
Contenzioso Amministrativo		X		X	Avvocatura	
Contenzioso Penale		X	X	X	Avvocatura	
Contenzioso Tributario		X		X	Avvocatura	
Contratti di lavoro dipendente/consulenze esterne	Lavoratori	X		X	Avvocatura	
Contratti di lavoro categorie protette	Lavoratori	X	X	X	Avvocatura	
Procedure di aggiudicazione lavori pubblici	Persone Fisiche e Giuridiche	X		X	Avvocatura	Ex lg 241/90
Procedure di aggiudicazione forniture di beni e prestazione di servizi	Persone Fisiche e Giuridiche	X		X	Avvocatura	Ex lg 241/90
Aste Pubbliche	Aziende, Cooperative, RTI, Studi Associati, Professionisti	X		X	Infrastrutture	Prefettura, Autorità sui lavori Pubblici, Cassa depositi e prestiti
Appalto Integrato		X		X	Infrastrutture	
Licitazioni Private		X		X	Infrastrutture	
Trattative Private		X		X	Infrastrutture	

Concessioni (Passi carrabili, occupazione suolo pubblico)	Persone Fisiche e Giuridiche, Enti Pubblici	X		X	Infrastrutture	
Espropri	Persone Fisiche e Giuridiche	X			Infrastrutture	
Scarichi nei corpi idrici	Persone Fisiche e Giuridiche	X			Pianificazione Territoriale - Ambiente	
Scarichi al suolo	Persone Fisiche e Giuridiche	X			Pianificazione Territoriale - Ambiente	
Denunce Pozzi	Persone Fisiche e Giuridiche	X			Pianificazione Territoriale - Ambiente	
Registro Imprese Trattamento riufiuti non pericolosi	Persone Fisiche e Giuridiche	X			Pianificazione Territoriale - Ambiente	
Approvazione PRG Comuni, Patiche Edilizie	Persone Fisiche e Giuridiche, Comuni	X			Pianificazione Territoriale - Urbanistica	
Rapporto nucleo di valutazione	Dirigenti	X	X		Ragioneria - Controllo Econ. e controllo di gestione	Corte dei Conti
Impegni sulla base di sentenze	Persone fisiche e giuridiche	X		X	Ragioneria - UO Impegni	
Impegni sulla base di cause di servizio - Indennizzi	Dipendenti	X	X		Ragioneria - UO Impegni	
Entrate	Persone fisiche e giuridiche	X			Ragioneria	
Spese	Persone fisiche e giuridiche	X			Ragioneria	
CED		X	X	X	Ragioneria	
Anagrafica	Enti e Comuni di riferimento	X			MARSEC	
Collocamento Lavoratori	Aspiranti Lavoratori	X	X	X	Centri per l'impiego	INPS, INAIL, Ispettorato del lavoro, Direzione Regionale del Lavoro
Anagrafica Aziende	Persone fisiche e giuridiche	X			Centri per l'impiego	

Tabella 1 - Elenco dei Trattamenti – Informazioni Essenziali

2.1. GENERALITÀ SUL SISTEMA INFORMATICO ATTUALE

Per la descrizione del sistema informatico attuale, la procedura d'accesso al sistema informativo e la gestione delle postazioni di lavoro si veda il documento "Istr_BN01-01", allegato e parte integrante del presente Documento Programmatico sulla Sicurezza.

3. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Per garantire la tutela dei dati personali e gestire la fase operativa d'adozione delle misure di sicurezza, la legge introduce (titolo IV), precisandone rispettivamente i poteri, i compiti e le responsabilità, le seguenti figure:

- Titolare del trattamento (art. 28)
- Responsabili del trattamento (facoltativi; art. 29)
- Incaricati del trattamento (art. 30)

3.1. TITOLARE

Ai sensi degli artt. 4, comma 1 lettera f, e 28 del d.lg. 196/03 il titolare del trattamento è la Provincia di Benevento nella persona del Presidente.

In particolare il Titolare:

- sovrintende a tutti gli adempimenti previsti dalla legge;
- impartisce ordini e direttive ai fini dell'osservanza delle norme vigenti in materia di riservatezza dei dati personali;
- adotta le misure e dispone gli interventi necessari per la sicurezza e la conservazione dei dati e per la correttezza dell'accesso;
- controlla che la comunicazione e l'eventuale diffusione dei dati avvenga nei limiti indicati dalla legge e dal presente regolamento;
- inoltra al Garante le richieste di autorizzazione al trattamento e le notificazioni previste dalla legge;
- designa, ove lo reputi necessario, uno o più responsabili del trattamento nel rispetto di quanto previsto dall'articolo 29, comma 1 del Testo Unico.

3.2. RESPONSABILE

Designati facoltativamente dal Titolare sono soggetti che, per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3.2.1. RESPONSABILI INTERNI

Al fine di rendere pervasiva l'applicazione della disciplina sulla privacy all'interno dell' Ente, il Titolare del trattamento ha ritenuto opportuno, ai sensi degli artt. 4, comma 1 lettera g e 29 del d.lg. 196/03, procedere, in funzione degli specifici profili professionali, alle seguenti nomine:

- Responsabili del trattamento dati: Dirigenti di Settore in relazione ai processi e alle funzioni svolte dai Settori di propria competenza;
- Responsabile del trattamento dei dati per gli aspetti informatici: Responsabile dei Sistemi informativi per i dati memorizzati su supporti informatici

RESPONSABILE DEL TRATTAMENTO	UNITA' ORGANIZZATIVA DI APPARTENENZA	TRATTAMENTI
dott.ssa Giovanna Romano	Mobilità ed energia	Trattamenti effettuati nel settore di competenza come da tabella 1
ing. Angelo d'Angelo	Pianificazione Territoriale	Trattamenti effettuati nel settore di competenza come da tabella 1
ing. Angelo Fuschini	Infrastrutture	Trattamenti effettuati nel settore di competenza come da tabella 1
ing. Valentino Melillo	Edilizia e Patrimonio	Trattamenti effettuati nel settore di competenza come da tabella 1
avv. Vincenzo Catalano	Avvocatura	Trattamenti effettuati nel settore di competenza come da tabella 1
dott. Sergio Muollo	Finanza (Ragioneria)	Trattamenti effettuati nel settore di competenza come da tabella 1
dott. Luigi Velleca	Politiche del lavoro	Trattamenti effettuati nel settore di competenza come da tabella 1
arch. Elisabetta Cuoco	Agricoltura	Trattamenti effettuati nel settore di competenza come da tabella 1
dott.ssa Alfonsina Colarusso	Personale	Trattamenti effettuati nel settore di competenza come da tabella 1
dott.ssa Patrizia Taranto	Servizi ai Cittadini	Trattamenti effettuati nel settore di competenza come da tabella 1
Dott. Ludovico Barone	UFFICIO SPECIALE MARSEC	Trattamenti effettuati nel settore di competenza come da tabella 1

Tabella 2 Responsabili Interni

I compiti dei Responsabili interni possono essere così riassunti:

- predisporre i processi organizzativi per la verifica delle misure di sicurezza che devono tenere conto dei rischi e delle misure minime disposte dal Testo Unico. In particolare le verifiche devono riguardare le aree di lavoro e gli strumenti di propria responsabilità;
- assicurare che il trattamento dei dati si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza ed all'identità personale;
- individuare, su richiesta del Titolare, gli Incaricati e predisporre delle istruzioni scritte;
- interagire per il tramite del Titolare con il Garante, in caso di richieste di informazioni o effettuazione di controlli ed accessi da parte dell'Autorità;
- informare preventivamente il Titolare qualora vengano istituiti nuovi trattamenti o si verifichino variazioni in ordine ai trattamenti già notificati;
- informare prontamente il Titolare di tutte le questioni rilevanti ai fini della Legge (ad es. richieste del Garante, esiti delle ispezioni delle Autorità, richieste degli interessati, ecc.);
- custodire e controllare i dati personali oggetto di trattamento, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

3.2.1.1. RESPONSABILE DEL TRATTAMENTO PER GLI ASPETTI INFORMATICI

E il soggetto cui è conferito il compito di sovrintendere alle risorse di sistema (rete, base di dati, elaboratore, applicazioni, ecc.) e di consentirne l'utilizzo.

Il Titolare ha nominato come Responsabile del Trattamento per gli aspetti Informatici:

Responsabile del trattamento per gli aspetti Informatici:
ING. SCARANO GIUSEPPE - RESPONSABILE SERVIZIO CED.

Tabella 3 Responsabile del Trattamento per gli aspetti Informatici

I compiti del Responsabile possono così essere riassunti:

- Verificare l'applicazione, sul sistema informativo nel quale risiedono le banche dati utilizzate per i trattamenti dei dati personali dell' Ente, delle misure indicate nel Disciplinare Tecnico del T.U.
- Verifica annuale della situazione delle apparecchiature hardware e relativi sistemi operativi e applicazioni installati con cui vengono trattati i dati, delle apparecchiature periferiche, ed in particolare dei dispositivi di collegamento con le reti pubbliche. La verifica ha lo scopo di controllare l'affidabilità del sistema per quanto riguarda:
  - La sicurezza dei dati trattati;
  - Il rischio di distruzione e perdita;

- Il rischio di accesso non autorizzato o non consentito;

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al salvataggio periodico degli stessi con copie di back-up;
- Assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi;
- Comunicare immediatamente qualsiasi elemento che possa compromettere o interferire il corretto trattamento dei dati personali.

3.2.2. RESPONSABILI ESTERNI

I responsabili esterni sono soggetti giuridicamente autonomi che svolgono in regime di outsourcing trattamenti di dati la cui titolarità spetta alla Provincia di Benevento.
Nel trattamento dei dati personali ai quali ha accesso, il Responsabile esterno dovrà attenersi alle istruzioni del Titolare comunicando tempestivamente allo stesso l'insorgere di eventuali problematiche non regolamentate in tema di trattamento di dati personali comuni e/o sensibili e/o giudiziari.

NOME SOCIETA'/LIBERO PROFESSIONISTA	AMBITO DI ATTIVITA'
...	...
...	...
...	...
...	...
...	...

Tabella 4 Responsabili esterni

I compiti dei responsabili esterni possono essere così riassunti:

- garantire che i dati personali siano raccolti con le modalità ed i requisiti richiesti dall'art. 11 del Codice ed in particolare:
  - che siano raccolti, registrati e trattati in modo lecito e corretto ed esclusivamente per gli scopi connessi alle finalità dell' Ente;
  - che tali dati siano esatti, aggiornati, pertinenti e non eccedenti rispetto agli scopi sopra enunciati e conservati in forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati, fermo restando, comunque il rispetto dei termini imposti dalle normative civilistiche e fiscali vigenti;

- effettuare i controlli necessari per accertare che i dati personali siano trattati in modo lecito, raccolti, registrati e trattati per gli scopi determinati, espliciti e legittimi, ed utilizzati con finalità e modalità conformi a quelle per le quali sono stati raccolti;

- mantenere la riservatezza dei dati che non devono essere comunicati o resi accessibili a terzi se non secondo le modalità concordate con il Titolare dei dati;

- collaborare con il Titolare per la predisposizione dell'informativa di cui all'art. 13 della Codice e richiedere il consenso dell'interessato (in forma scritta qualora si tratti di dati sensibili), ove necessario;

- individuare e dare agli Incaricati autorizzati al trattamento le istruzioni scritte necessarie per un corretto, lecito e sicuro trattamento;

- vigilare e controllare il trattamento svolto dagli Incaricati;

- predisporre, rispettare e applicare procedure adeguate per l'adozione di Misure di Sicurezza idonee a salvaguardare la riservatezza, l'integrità e la completezza dei dati trattati, secondo quanto disposto negli artt. 33, 34 e 35 e nel Disciplinare Tecnico in materia di Misure Minime di Sicurezza;

- attenersi in ogni caso alle istruzioni del Titolare.

3.3. INCARICATI

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione personale per iscritto da parte del Titolare o del Responsabile del trattamento, con la quale si individua l'ambito del trattamento consentito.

Di seguito si riporta la lista completa degli Incaricati e della relativa area operativa di competenza:

SETTORE	Responsabile del trattamento	NOMINATIVO	PROFILO PROFESSIONALE
EDILIZIA E PATRIMONIO	MELILLO Valentino	PANARESE Michelantonio	Istruttore direttivo esperto tecnico
		BALLARINO Giancarlo	Istruttore direttivo tecnico
		DE MICHELE Nicola	Istruttore direttivo tecnico
		DI DIO Aldo	Istruttore direttivo tecnico
		FRESTA Roberto	Istruttore direttivo tecnico
		MERVOGLINO Francesco	Istruttore direttivo tecnico
		RUBBO Sergio	Istruttore direttivo tecnico
		CLARIZIA Giovanna	Istruttore direttivo economic/finanz.
		DE BELLIS Serafino	Istruttore direttivo amm.vo
		CALABRESE Cosimo	Istruttore tecnico
		CAPORASO Gaetano	Istruttore tecnico
		FUCCI Carolina	Istruttore amm.vo
		GENITO Serafino	Istruttore tecnico
		BORRELLI Paola	Istruttore direttivo tecnico

		PISCITELLI Luigi	Istruttore tecnico
		SATERIALE Antonio	Istruttore tecnico
		MALFI Antonio	Responsabile Parco Auto
		COPPOLA Raffaele	Esecutore tecnico
		MAIO Nicola	Esecutore amm.vo
		SANGIUOLO Cosimo	Esecutore tecnico cond.macch.oper.
		VALENTI Salvatore	Esecutore amm.vo
		TOMACIELLO Rita	Operatore Servizi Ausiliari
		CASSETTA Giorgio	Operatore Servizi Ausiliari
		OCONE Silvio	Istruttore direttivo tecnico
FINANZA E CONTROLLO ECONOMICO	MUOLLO Sergio	BRUNO Vincenzo	Istruttore direttivo esperto econ./fin.
		BACCARI Silvio	Istruttore direttivo econ./finanz.
		CREDENDINO Fortuna	Istruttore direttivo econ./finanz.
		CRETA Giuseppe	Istruttore direttivo econ./finanz.
		D'AMELIA Vincenzo	Istruttore direttivo econ./finanz.
		GIARDIELLO Giovanni	Istruttore direttivo econ./finanz.
		PANNELLA Gabriella	Istruttore direttivo econ./finanz.
		DELL'ORZO Anna	Istruttore Informatico
		DE VIZIA Maria Paola	Istruttore econ./finanz.
		ROSSI Katiuscia	Istruttore econ./finanz.
		MANGANIELLO Annamaria	Istruttore amm.vo
		MENNITTO Giovanna	Istruttore amm.vo
		DE PIANO Nicola	Esecutore amm.vo
		MISIANO Maria Rosaria	Esecutore amm.vo
		CARBONE Rossana	Esecutore amm.vo
		LANNI Antonio	Operatore Servizi Ausiliari
		SORICELLI Luigi	Operatore Servizi Ausiliari
		MICELI Silvia	Istruttore econ./finanz.
AGRICOLTURA-ALIMENTAZIONE	CUOCO Elisabetta	DI GIAMBATTISTA Pasquale	Istruttore direttivo tecnico
		LUCIANI Rita	Istruttore direttivo amm.vo
		PORCARO Giuseppe	Istruttore direttivo tecnico
		RENZI Bernanrdino	Istruttore direttivo tecnico
		BARONE Giovanni	Istruttore amm.vo
		DANIELE Michele	Istruttore amm.vo
		DI MARTINO Vincenzo	Istruttore amm.vo
		MORELLI Nicola	Istruttore amm.vo
		PETRONZI Pasquale	Istruttore econ./finanz.
		RILLO Virgilia	Istruttore amm.vo
		DE LAURO Ignazio	Esecutore tecnico
		DI VIZIO Alfredo	Esecutore amm.vo
		FINELLI Francesco	Esecutore amm.vo
		SALVATORE Francesco	Esecutore amm.vo
		D'AVOLIO Geda	Opertaore servizi ausiliari

		TASSELLA Lorenzo	Opertaore servizi ausiliari
		CASTELLUCCI Antonio	Istruttore direttivo tecnico
		POCINO Franco	Istruttore direttivo tecnico
		LAUDATO Rocco	Istruttore tecnico
AVVOCATURA PROVINCIALE	CATALANO Vincenzo	VOLPE Candido	Istruttore direttivo esperto legale
		FRANCO Armando	Istruttore direttivo amm.vo
		D'UVA Serafina	Istruttore direttivo amm.vo
		MIRRA Antonetta	Istruttore amm.vo
		CESARE Rita	Esecutore amm.vo
		CASSETTA Salvatore	Esecutore amm.vo
		CAMPANA Angela	Operatore servizi ausiliari
SERVIZI AI CITTADINI	TARANTO Patrizia	BURATTO Antonio	Istruttore direttivo esperto amm.vo
		DEL GROSSO Libera	Istruttore direttivo esperto amm.vo
		NAZZARO Michele	Istruttore direttivo esperto econ./finanz.
		BARTOLOMEI Luigina	Istruttore direttivo amm.vo
		CASILLO Serafina	Istruttore direttivo amm.vo
		DE FELICE Concetta	Istruttore direttivo amm.vo
		DE LUCIA Antonio	Istruttore direttivo amm.vo
		INSOGNA Luigi	Istruttore direttivo amm.vo
		MARTONE Grazia	Istruttore direttivo amm.vo
		SFORZA Rosanna	Istruttore direttivo amm.vo
		CAPOCASALE Fortunato	Istruttore amm.vo
		FICOCIELLO Loredana	Istruttore amm.vo
		LABAGNARA Carmela	Istruttore econ./finanz.
		MIRRA Carlo	Istruttore amm.vo
		PADUANO Vincenzo	Istruttore amm.vo
		PIANTADOSI Ornella	Istruttore amm.vo
		POZZUTO Pasqualina	Istruttore amm.vo
		SCHIPANI Angelo	Istruttore amm.vo
		SICILIANO Anna Maria	Istruttore amm.vo
		VALENTE Maria Concetta	Istruttore amm.vo
		CAPORASO Vincenza	Esecutore amm.vo
		CORRADO Raffaele	Esecutore amm.vo
		DE CRISTOFARO Alessandro	Esecutore amm.vo (messo notif.)
		FUCCI Annamaria	Esecutore amm.vo
		NAZZARO Immacolata	Esecutore amm.vo
		SARRACINO Tullio	Coordinatore autista
		TROISE Giuseppina	Esecutore amm.vo
		VIVOLO Palmina	Esecutore amm.vo

		ZAMPETTI Pasquale	Esecutore amm.vo
		CAPPELLETTI Carmine	Operatore servizi Ausiliari
		CERNIERI Filomena	Operatore servizi Ausiliari
		GAROFANO Angela Rita	Operatore servizi Ausiliari
		LEPORE Maria	Operatore servizi Ausiliari
		PISANO Carmela	Operatore servizi Ausiliari
		SANTANIELLO Valerio	Operatore servizi Ausiliari
		MAGLIONE Cosimo	Esecutore amm.vo
		FISCHETTI Giovanni	Operatore servizi Ausiliari
		De Santis Maria	Istruttore direttivo amm.vo
		Boscaino Armando	Istruttore amm.vo
		D'Aronzo Giovanni	Istruttore amm.vo
		Di Giuseppe Carmine	Istruttore amm.vo
		Grillo Vincenzo	Istruttore amm.vo
		Miele Antonio	Istruttore amm.vo
		Principe Claudio Mosè	Istruttore amm.vo
		Solano Fabio	Istruttore amm.vo
		Somma Leonida	Istruttore amm.vo
		Tanzillo Alessandro	Istruttore amm.vo
		ROMANO Osvaldo	Istruttore direttivo amm.vo
		AUDI Nicolina	Istruttore econ./finanz.
		BARBIERI Maria Lucia	Istruttore culturale
		D'AGOSTINO Anna	Istruttore culturale
		LAPALORCIA Maria Rosaria	Istruttore culturale
		MASCIA Adelina	Istruttore culturale
		CIRNELLI Patrizia	Esecutore culturale
		TIZZANINO Antonio	Coordinatore servizi ausiliari
		VESSICHELLI Arturo	Esecutore tecnico
		AGRIPPO Aniello	Operatore servizi Ausiliari
		DE GIROLAMO Giuseppina	Operatore servizi Ausiliari
		FORNARI Rita	Operatore servizi Ausiliari
		LANZOTTI Francisco Rafael	Operatore servizi Ausiliari
		POSSEMATO Concetta	Operatore servizi Ausiliari
		FICOCIELLO Silvana	Istruttore culturale
		MATARAZZO Adele	Istruttore culturale
		MOGAVERO Alessandra	Istruttore culturale
		PERROTTA Giuseppa	Istruttore culturale
INFRASTRUTTURE	FUSCHINI Angelo	CARUSO Francesco	Istruttore direttivo esperto tecnico
		FELEPPA Antonio	Istruttore direttivo esperto amm.vo
		MINICOZZI Salvatore	Istruttore direttivo esperto tecnico
		PAPA Alessandrina	Istruttore direttivo esperto tecnico
		TRAVAGLIONE Augusto	Istruttore direttivo esperto tecnico

		~~BORRELLI Paola~~	~~Istruttore direttivo tecnico~~
		CIARLO Giuseppe	Istruttore direttivo tecnico
		D'ABROSCA Dino	Istruttore direttivo tecnico
		DE BLASIO Angelo	Istruttore direttivo tecnico
		GALLO Liberato	Istruttore direttivo tecnico
		PEPICIELLO Biagio	Istruttore direttivo tecnico
		RISPOLI Stefania	Istruttore direttivo tecnico
		COMOLETTI Giuseppina	Istruttore direttivo amministrativo
		PERFETTO Antonio	Istruttore direttivo amministrativo
		IANNACE Tiziana	Istruttore direttivo economico/finanz
		CAPUOZZO Giuseppe	Istruttore tecnico
		CARACCIO Mario	Istruttore tecnico
		CUSANO Enrico	Istruttore tecnico
		MARCARELLI Giancarlo	Istruttore tecnico
		MIGNONE Nazzareno	Istruttore tecnico
		PALOMBINO Giovanni	Istruttore tecnico
		RAFFA Guido	Istruttore tecnico
		RANDELLI Carmine	Istruttore tecnico
		ROMANO Roberto	Istruttore tecnico
		AMABILE Gaetano	Istruttore amministrativo
		CALABRESE Annamaria	Istruttore amministrativo
		FUSCO Rosa Maria	Istruttore amministrativo
		RICCIARDI Raffaella	Istruttore amministrativo
		ESPOSITO Pietro	Responsabile squadre operat. Viabilità
		SABATINO Angelo	Responsabile squadre operat. Viabilità
		VARRICCHIO Carmine	Responsabile squadre operat. Viabilità
		VENDITTI Salvatore	Responsabile squadre operat. Viabilità
		FRONGILLO Giovanni	Esecutore tecnico addetto alla viabilità
		LEPORE Gerardo	Esecutore tecnico addetto alla viabilità
		MAGGIO Luigi	Esecutore tecnico cond. macch. oper.
		NIGRO Giocondo	Esecutore tecnico addetto alla viabilità
		ARAMINI Rosalba	Esecutore amministrativo
		CARUSO Immacolata	Esecutore amministrativo
		PARENTE Germano	Esecutore amministrativo
		LARRUSSO Francesco	Operatore Servizi ausiliari
		DE MATTEO Filippo	Operatore Tecnico
		MASELLI Francesco	Operatore Tecnico
		PELOSI Luigi	Operatore Tecnico
		PONTE Saverio	Operatore Tecnico
		ROSSI Arsenio	Operatore Tecnico
		SCOTECE Antonio	Operatore Tecnico
UFFICIO SPECIALE MARSEC	BARONE Ludovico	NAPOLITANO Annamaria	Istruttore direttivo amm.vo

MOBILITA' ENERGIA	ROMANO Giovanna	PISANIELLO Elio	Istruttore direttivo esperto tecnico
		BIANCO Bruno	Istruttore direttivo tecnico
		BUCCIANO Fernando	Istruttore direttivo amministrativo
		IULIANO Vincenzo	Istruttore direttivo amministrativo
		CERMOLA Pasquale	Istruttore tecnico
		IESCE Salvatore	Istruttore tecnico
		CAPOBIANCO Marcello	Istruttore amministrativo
		GUARENTE Maria Rosa	Istruttore amministrativo
		MENNITTO Patrizia	Istruttore amministrativo
		ESPOSITO Margherita	Esecutore amministrativo
		SIGNORIELLO Gianpaolo	Istruttore direttivo tecnico
		CAPORASO Nicola	Esecutore tecnico
PIANIFICAZIONE TERRITORIALE	D'ANGELO Angelo	ARGENIO Vincenzo	Istruttore direttivo esperto tecnico
		COLANTUONI Anna	Istruttore direttivo esperto amm.vo
		MOSCARINO Carlo	Istruttore direttivo esperto tecnico
		D'AGOSTINO Giovanni Francesco	Istruttore direttivo amm.vo
		MONGILLO Fernando	Istruttore direttivo amm.vo
		FUSCO Gennaro	Istruttore direttivo tecnico
		DELL'OMO Umberto	Istruttore tecnico
		GOGLIA Mariano	Istruttore tecnico
		LA PIETRA Genoveffa	Collaboratore profess. Terminalista
		RANAURO Antonio	Esecutore tecnico
		MUCCI Tonino	Operatore Servizi Ausiliari
		CASERTA Carlo	Istruttore tecnico
POLITICHE ATTIVE DEL LAVORO	VELLECA Luigi	GOMMA Gabriella	Istruttore direttivo esperto amm.vo
		MARSICANO Giuseppe	Istruttore direttivo esperto amm.vo
		PESCITELLI Luigi	Istruttore direttivo esperto amm.vo
		BELLICOSA Anna Maria	Istruttore direttivo amm.vo
		BOFFA Maria	Istruttore direttivo amm.vo
		ESPOSITO Giovanni	Istruttore direttivo amm.vo
		GALASSO Giuseppe	Istruttore direttivo amm.vo
		IANNOTTA Luca	Istruttore direttivo amm.vo
		LEPORE Ernesto	Istruttore direttivo amm.vo
		MOLLICA Anna Maria	Istruttore direttivo amm.vo
		LOMBARDI Nino	Istruttore direttivo amm.vo

SORICE Rosalba	Istruttore direttivo amm.vo
VENTURA Giuseppe	Istruttore direttivo amm.vo
BOSCO Brigida	Istruttore amm.vo
BUONO Mario	Istruttore amm.vo
CAMPAGNUOLO Vittorio	Istruttore amm.vo
CARUSO Gerardo	Istruttore amm.vo
CATILLO Dolorisa	Istruttore amm.vo
CAVALUZZO Angelo	Istruttore amm.vo
DE RIENZO Franca	Istruttore amm.vo
DEL VECCHIO Angela	Istruttore amm.vo
IATOMASI Iolanda	Istruttore amm.vo
LANDI Giuseppe	Istruttore amm.vo
ROSSI Emilia	Istruttore amm.vo
MASTRONARDI Antonio	Istruttore amm.vo
MELE Annamaria	Istruttore amm.vo
SETARO Alfonso	Istruttore amm.vo
ZAPPAVIGNA Anna Maria	Istruttore amm.vo
AMORIELLO Rita	Collaboratore professionale amm.vo
BIANCO Dionigio	Collaboratore professionale amm.vo
BOSCO Grazia Rosaria	Collaboratore professionale amm.vo
BOTTICELLA Rita	Collaboratore professionale amm.vo
CARUSO Donata	Collaboratore professionale amm.vo
CIABRELLI Rosa Maria	Collaboratore professionale amm.vo
CIARDIELLO Rosa	Collaboratore professionale amm.vo
CORSINI Ernesto	Collaboratore professionale amm.vo
CUSANI Anna Maria	Collaboratore professionale amm.vo
DE BLASIO Carmela	Collaboratore professionale amm.vo
DE LIBERO Emanuele	Collaboratore professionale amm.vo
DE NIGRIS Assunta	Collaboratore professionale amm.vo
DE NISI Mario	Collaboratore professionale amm.vo
DEL VECCHIO Luigi Pietro	Collaboratore professionale amm.vo
DIODATO Pasquale	Collaboratore professionale amm.vo
FERRANTE Amalia	Collaboratore professionale amm.vo
FULGIERI Antonietta	Collaboratore professionale amm.vo
IACICCO Immacolata	Collaboratore

			professionale amm.vo
		IAMMARINO Antonia	Collaboratore professionale amm.vo
		IANNOTTA Maria Antonia	Collaboratore professionale amm.vo
		IMBELLI Cosimo	Collaboratore professionale amm.vo
		LONGO Franco	Collaboratore professionale amm.vo
		MAINIERO Giuseppe	Collaboratore professionale amm.vo
		MELOTTA Ciro	Collaboratore professionale amm.vo
		MIGNONE Carmine	Collaboratore professionale amm.vo
		ORSILLO Rosa Maria	Collaboratore professionale amm.vo
		PALLADINO Carmela	Collaboratore professionale amm.vo
		PITEO Lucia	Collaboratore professionale amm.vo
		RAUCCI Carlo	Collaboratore professionale amm.vo
		RINALDI Antonietta	Collaboratore professionale amm.vo
		ROTONDO Emanuele	Collaboratore professionale amm.vo
		FORGIONE Orazio	Esecutore amm.vo
		LANNI Filomena	Esecutore amm.vo
		MATTO Claudio	Esecutore amm.vo
		PALUMBO Anna Maria	Esecutore amm.vo
		TRETOLA Rita	Esecutore amm.vo
		SORICELLI Luigi	Operatore servizi ausiliari
		PICA Pietro	Istruttore direttivo amm.vo
		DE PIERRO Giovanni	Istruttore amm.vo
RISORSE UMANE	COLARUSSO Alfonsina	COLABELLO Maria Antonietta	Istruttore direttivo esperto econ./fin.
		CARETTI Giorgio	Istruttore direttivo econ./finanz.
		RUSSO Agostino	Istruttore direttivo econ./finanz.
		IZZO Antonio	Istruttore direttivo amm.vo
		LEGGIERI Cosimo	Istruttore direttivo amm.vo
		MARTIGNETTI Rito	Istruttore direttivo amm.vo
		PICCIRILLO Antonio	Istruttore direttivo amm.vo
		DI MARIA Angela	Istruttore amm.vo
		FERRARA Vitangela	Istruttore econ./finanz.
		SORECA Maurizio	Istruttore econ./finanz.
		MARCHETTI Nicola	Istruttore informatico
		CARPENTIERI Carla	Istruttore amm.vo
		MERONE Maria Fiorella	Istruttore amm.vo

		IOVINO Maria Grazia	Istruttore amm.vo
		CUSANO Antonietta	Esecutore amm.vo
		GIARDIELLO Eleonora	Esecutore amm.vo
		GIULIANO Lucia	Esecutore amm.vo
		ITRO Maria Teresa	Centralinista non vedente
		MARGHERINI M.Gabriella	Esecutore amm.vo
		ROSSI Eugenio	Centralinista non vedente
		SORTINO Salvatore	Esecutore amm.vo
		CARPENITO Assunta	Operatore servizi Ausiliari
		FUSCO MARIA PIA	Operatore servizi Ausiliari
		NAPOLITANO Antonia	Operatore servizi Ausiliari
		D'ONOFRIO Carmine	Esecutore amm.vo
		PAVONE Antonio	Centralinista non vedente
		CATALANO Giovanni	Istruttore direttivo specialista vigilanza
		FIORITO Vincenzo	Istruttore direttivo specialista vigilanza
		MONGILLO Gabriella	Istruttore direttivo specialista vigilanza
		BOSCO Giuseppe	Istruttore vigilanza
		BOZZI Raffaele	Istruttore vigilanza
		CIRCELLI ANTONIO	Istruttore vigilanza
		DEL GIUDICE Camillo	Istruttore vigilanza
		DE PASCALE Soccorso	Istruttore vigilanza
		DI MARIA Giuseppe	Istruttore vigilanza
		ESPOSITO Giancarlo	Istruttore vigilanza
		FUSCO Gabriele	Istruttore vigilanza
		MAROTTI Filippo	Istruttore vigilanza
		MASTROCOLA Nicola	Istruttore vigilanza
		PAOLETTI Michele	Istruttore vigilanza
		PARRELLA Angelo	Istruttore vigilanza
		RAPUANO Michelino	Istruttore vigilanza
		RILLO Vincenzo	Istruttore vigilanza
		RUSSO Gianfranco	Istruttore vigilanza
		TIRELLI Carlo Alberto	Istruttore vigilanza
		VITIELLO Nicola	Istruttore vigilanza
		PUGLIESE Franco	Istruttore amm.vo
		DE VITA Silvana	Collaboratore profess. Terminalista

E' stato individuato un ambito del trattamento consentito agli incaricati in relazione ad ogni specifico Settore di appartenenza.

I compiti degli incaricati possono così essere riassunti:

- accedere ai soli dati necessari e sufficienti all'esercizio delle operazioni di trattamento contrattualmente definite ed effettuate nel settore di competenza;
- osservare le misure di protezione e sicurezza già in atto e quelle che successivamente verranno disposte, atte ad evitare rischi di perdita, accesso non autorizzato o trattamento non consentito;

- non utilizzare o trasmettere mai nessun dato personale all'esterno in qualunque forma, sia come comunicazione che come diffusione, senza la preventiva autorizzazione del titolare o del responsabile. In qualsiasi caso, la comunicazione di dati personali dovrà essere fatta garantendo riservatezza e sicurezza della circolazione, fatti salvi i diritti dell'interessato;
- comunicare tempestivamente al titolare o al responsabile l'insorgere di eventuali problematiche non regolamentate in tema di trattamento dei dati personali, comuni o sensibili.

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati sono fornite esplicite istruzioni relativamente a:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli comuni e sensibili, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie ,per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola chiave;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro;
- procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimuovibili contenenti dati personali;

3.3.1. CUSTODE DELLE CREDENZIALI DI AUTENTICAZIONE

Quando l'accesso ai dati memorizzati sugli elaboratori elettronici è consentito solamente mediante l'utilizzo della componente riservata della credenziale di autenticazione (password), anche al fine di assicurare la disponibilità dei dati in caso di impedimento o assenza dell'incaricato, il Titolare del trattamento nomina un custode delle credenziali di autenticazione:

CUSTODE DELLE CREDENZIALI
Nome Custode

Tabella 5 Custode delle credenziali

In particolare all'incaricato preposto alla custodia delle credenziali di autenticazione sono attribuiti i seguenti compiti:

- prendere conoscenza, laddove necessario, dagli incaricati del trattamento dei dati personali con elaboratori elettronici, delle credenziali di autenticazione per l'accesso agli stessi;
- custodire le credenziali di autenticazione attribuite dagli incaricati del trattamento di dati personali con elaboratori elettronici;
- nel caso in cui il titolare del trattamento abbia la necessità indifferibile di accedere ad un elaboratore in caso di prolungata assenza o impedimento dell'incaricato che lo utilizza

abitualmente, consegnare al titolare stesso la parola chiave dell'elaboratore sul quale egli può intervenire unicamente per necessità di operatività e sicurezza del sistema informativo;

- informare tempestivamente l'incaricato del quale, in sua assenza, sono state consegnate le credenziali di autenticazione al titolare del trattamento, affinché questi provveda immediatamente alla loro sostituzione.
- attenersi ad un generale dovere di non divulgazione dei dati trattati o di quelli di cui sia venuto a conoscenza tramite altre fonti.

4. MISURE DI SICUREZZA ADOTTATE

Le misure di sicurezza (minime e idonee) che la Provincia di Benevento ha adottato sono state scelte con riferimento a criteri e procedure tecniche e organizzative, rivolte a ridurre al minimo i rischi di distruzione o di perdita anche accidentale dei dati, di accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

Tali misure sono classificate in due categorie:

- misure di sicurezza minime e idonee associate ai trattamenti **con l'ausilio di strumenti elettronici**;
- misure di sicurezza minime e idonee associate ai trattamenti **senza l'ausilio di strumenti elettronici**.

4.1. TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Nelle tabelle che seguono è riportato il grado di copertura dell' Ente in relazione alle misure di sicurezza associabili (Tabella 6) e non associabili (Tabella 7) alle banche dati, relativamente ai trattamenti svolti con l'ausilio di strumenti elettronici.

In particolare ogni tabella contiene i seguenti campi:

- **Riferimento al T.U.:** contiene il riferimento all'articolo del Disciplinare Tecnico del Testo Unico nel quale sono esplicitate le misure di sicurezza previste dalla Legge;
- **Misure di sicurezza:** contiene la descrizione delle misure minime di sicurezza contenute nel corrispondente articolo del Disciplinare Tecnico del T.U. e la descrizione delle misure idonee per la protezione delle aree e dei locali;

- **Grado di copertura:**
  - per le misure di sicurezza associate alle banche dati: il grado di copertura equivale alla completa adozione (100%), parziale adozione (50%) o meno (0%) della misura di sicurezza nell' Ente;
  - per le misure di sicurezza non associabili alle banche dati: il grado di copertura equivale alla completa adozione (100%), parziale adozione (50%) o meno (0%) della misura di sicurezza nell' Ente;
  - nel caso in cui non esistano le condizioni per l'applicabilità della misura di sicurezza sarà riportata la dicitura "N.a.", cioè non applicabile.

4.1.1. MISURE DI SICUREZZA ASSOCIATE ALLE BANCHE DATI

Tipologia di Misura	Riferimento Testo Unico	Misure "Minime" di sicurezza Trattamenti effettuati con l'ausilio di strumenti elettronici	Misura già in essere	
Sistema di autenticazione informatica				
Sistema di Autenticazione	Disciplinare Tecnico n° 2	Assegnazione ad ogni incaricato di una o più credenziali di autenticazione che consenta il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti	50	
Sistema di Autenticazione	Disciplinare Tecnico n° 2	Credenziali di autenticazione conosciute solo dall'incaricato e ad esso univocamente correlate		50
Sistema di Autenticazione	Disciplinare Tecnico n° 7	Disattivazione delle credenziali di autenticazione non utilizzate da almeno 6 mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (es utilizzate dagli amministratori di sistema)		0
Sistema di Autenticazione	Disciplinare Tecnico n° 8	Disattivazione delle credenziali nel caso in cui l'incaricato perda la qualità (ruolo/compito) per l'accesso ai dati personali		0
Sistema di Autenticazione	Disciplinare Tecnico n° 5	Parola chiave, quando prevista dal sistema di autenticazione, composta da almeno 8 caratteri		0
Sistema di Autenticazione	Disciplinare Tecnico n° 5	Parola chiave composta da un numero di caratteri pari al massimo consentito (nel caso in cui lo strumento elettronico non permetta la creazione di password di 8 caratteri)		0
Sistema di Autenticazione	Disciplinare Tecnico n° 5	Modifica della parola chiave da parte degli Incaricati al primo utilizzo		50
Sistema di Autenticazione	Disciplinare Tecnico n° 5	Modifica della parola chiave, nel caso di trattamenti di dati comuni, da parte degli Incaricati almeno ogni 6 mesi		0
Sistema di Autenticazione	Disciplinare Tecnico n° 5	Modifica della parola chiave, nel caso di trattamento di dati sensibili e di dati giudiziari, almeno ogni 3 mesi		0
Sistema di Autenticazione	Disciplinare Tecnico n°6	Codice per l'identificazione, laddove usato, non è assegnato ad altri incaricati, neppure in tempi diversi		0
Sistema di autorizzazione				
Sistema di Autorizzazione	Disciplinare Tecnico n° 12	Sistema di autorizzazione nel caso in cui siano previsti per gli incaricati più profili di autorizzazione con ambiti diversi	si	

Sistema di Autorizzazione	Disciplinare Tecnico n° 13	Individuazione e configurazione prima dell'inizio del trattamento dei profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati		50
Sistema di Autorizzazione	Disciplinare Tecnico n° 14	Verifica periodica (almeno annuale) della sussistenza delle condizioni per la conservazione dei profili di autorizzazione		0
Altre misure di sicurezza				
Altre misure di sicurezza	Disciplinare Tecnico n°16	Implementazione di strumenti elettronici per garantire la protezione dei dati personali contro il rischio di intrusione (Firewall) e dell'azione di virus o software dannosi (Antivirus)	100	
Altre misure di sicurezza	Disciplinare Tecnico n°16	Aggiornamento di tali strumenti con cadenza almeno semestrale		100
Altre misure di sicurezza	Disciplinare Tecnico n°17	Aggiornamento dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti (es. SERVICE PACK E PATCHES) almeno annuale	100	
Altre misure di sicurezza	Disciplinare Tecnico n°17	Aggiornamento di questi sw, in caso di trattamento di dati sensibili o giudiziari, almeno semestrale		100
Ulteriori misure in caso di trattamento di dai sensibili e giudiziari				
Tipologia di Misura	**Riferimento Testo Unico**	**Misure "Idonee" di sicurezza Trattamenti effettuati con l'ausilio di strumenti elettronici**		
Idonea	/	Esiste un servizio di vigilanza per il CED	0	
Idonea	/	Esiste un servizio di videosorveglianza nel CED	0	
Idonea	/	Sistemi di allarme e/o antintrusione nel CED	0	
Idonea	/	Sistemi antincendio nel CED	50	
Idonea	/	Effettuazione di controlli periodici sui sistemi antincendio	50	
Idonea	/	Sistemi di rilevazione fumi nel CED	100	
Idonea	/	Impianto di antiallagamento nel CED	0	
Idonea	/	Gruppi di continuità elettrica per i server	100	
Idonea	/	La sala macchine è chiusa a chiave in assenza di personale	100	
Idonea	/	Nomina di custodi delle chiavi dei locali in cui si trovano gli strumenti elettronici	100	
Idonea	/	Log delle attività svolte dagli incaricati mediante un'applicazione	0	
Idonea	/	Presenza di una persona che controlla periodicamente i log delle applicazioni	0	
Idonea	/	Adozione di un software per la gestione in automatico delle utenze	50	
Idonea	/	Custodia dei supporti (es. di backup) in contenitori ignifughi	0	
Idonea	/	Custodia dei supporti di backup in luoghi diversi da quelli in cui si trovano i computer in cui sono memorizzati i dati	0	
Idonea	/	Effettuazione periodica di test di verifica delle vulnerabilità del sistema server su cui risiede la banca dati	0	
Idonea	/	Aggiornamento tempestivo delle vulnerabilità del sistema operativo	100	
Idonea	/	Esistenza di documentazione aggiornata sulle configurazioni dei database/server/applicativi	0	

Idonea	/	Effettuazione di configurazioni di sicurezza per la protezione del sistema e dei dati ivi contenuti (ad es. attivo il File System NTFS, effettuato hardening del sistema operativo, ecc.)	100

Tabella 6 Misure di sicurezza minime e idonee relative ai trattamenti con l'ausilio di strumenti elettronici direttamente associate alle banche dati

4.1.2. MISURE DI SICUREZZA NON ASSOCIATE ALLE BANCHE DATI

Tipologia di Misura	Rif. Testo Unico	Misure "Minime" di sicurezza Trattamenti effettuati con l'ausilio di strumenti elettronici	Misura già in essere	
Sistema di autenticazione informatica				
Sistema di Autenticazione	Disciplinare Tecnico n° 4	Esistenza di specifiche istruzioni scritte rilasciate agli incaricati, in cui è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale (password)	100	
Sistema di Autenticazione	Disciplinare Tecnico n° 5	Formalizzazione del divieto di comporre la parola chiave con riferimenti agevolmente riconducibili all'incaricato (es. nome, data di nascita, nomi di familiari)	100	
Sistema di Autenticazione	Disciplinare Tecnico n° 9	Esistenza di specifiche istruzioni scritte rilasciate agli incaricati in cui è prescritto di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento	100	
Sistema di Autenticazione	Disciplinare Tecnico n° 10	Esistenza di disposizioni che individuano le modalità con le quali il Titolare può assicurare, in caso di necessità operativa, la disponibilità dei dati o degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato	100	
Sistema di Autenticazione	Disciplinare Tecnico n° 10	Individuazione per iscritto dei soggetti incaricati della custodia delle credenziali di autenticazione nel caso in cui sia tecnicamente impossibile garantire l'accesso ai dati senza l'utilizzo della componente riservata delle credenziali di autenticazione (password)		100
Sistema di Autenticazione	Disciplinare Tecnico n° 10	Formalizzazione di procedure che disciplinino la custodia delle copie delle credenziali garantendo la massima segretezza		100
Sistema di Autenticazione	Disciplinare Tecnico n° 10	Definizione di procedure che disciplinano le modalità operative per informare tempestivamente l'incaricato circa l'utilizzo della propria credenziale di autenticazione per l'accesso al sistema in sua assenza		100
Altre misure di sicurezza				
Altre misure di sicurezza	Disciplinare Tecnico n° 15	Aggiornamento periodico (almeno annualmente) della lista degli incaricati e degli addetti alla gestione/manutenzione degli strumenti elettronici e del relativo ambito del trattamento dei dati personali	0	
Altre misure di sicurezza	Disciplinare Tecnico n° 18	Esistenza di istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale	100	
Documento Programmatico sulla Sicurezza				
DPS	Disciplinare Tecnico n°19	Redazione del Documento Programmatico sulla Sicurezza nell'ipotesi di trattamenti di dati sensibili e giudiziari	si	

DPS	Disciplinare Tecnico n°19	Aggiornamento del documento entro il 31 marzo di ogni anno		si
DPS	Disciplinare Tecnico n°19	Analisi dei rischi		si
DPS	Disciplinare Tecnico n°19	Piano di formazione per gli incaricati		si
DPS	Disciplinare Tecnico n°19	Adozione di criteri per garantire l'adozione di misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare (OUTSOURCING)		si
Ulteriori misure in caso di trattamento di dati sensibili e giudiziari				
Sensibili e Giudiziari	Disciplinare Tecnico n°21	Esistenza di istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati (sensibili e giudiziari) al fine di evitare accessi non autorizzati e trattamenti non consentiti	100	
Sensibili e Giudiziari	Disciplinare Tecnico n°22	I supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, sono distrutti o resi inutilizzabili	0	
Sensibili e Giudiziari	Disciplinare Tecnico n°22	I supporti rimovibili contenenti dati sensibili o giudiziari vengono riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, esclusivamente nell'ipotesi in cui le informazioni non siano intelligibili e tecnicamente in alcun modo recuperabili	0	
Sensibili e Giudiziari	Disciplinare Tecnico n°23	Sono state adottate idonee misure e specifiche procedure per garantire il ripristino dell'accesso ai dati (sensibili e giudiziari) in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati (max 7gg)	0	
Misure di tutela e garanzia				
Misure di tutela e garanzia	Disciplinare Tecnico n°25	Qualora ci si avvalga di soggetti esterni alla propria struttura per adottare misure minime di sicurezza si richiede all'installatore una descrizione scritta dell'intervento effettuato che n' attesta la conformità alle disposizioni del presente disciplinare	50	
Misure di tutela e garanzia	Disciplinare Tecnico n°26	Nella relazione accompagnatoria del bilancio (se dovuta), il titolare riferisce l'avvenuta redazione o aggiornamento del Documento Programmatico sulla Sicurezza	100	
	Riferimento Testo Unico	**Misure "Idonee" di sicurezza Trattamenti effettuati con l'ausilio di strumenti elettronici**		
Misure Idonee	/	Accesso agli edifici controllato da un servizio di guardia/portineria	0	
Misure Idonee	/	Verifiche della leggibilità dei supporti di backup	0	
Misure Idonee	/	Apparecchiature installate in aree chiuse o protette (server, gateway, router)	50	
Misure Idonee	/	Dispositivi per la limitazione dell'accesso a particolari siti web potenzialmente pericolosi (black list)	0	
Misure Idonee	/	Dispositivi per la sospensione temporanea o definitiva (previo intervento dell'amministratore di sistema) dell'accesso, dopo la digitazione errata per n volte della password	0	
Misure Idonee	/	Predisposizione di linee e/o numeri dedicati per la trasmissione di dati sensibili , con limitazioni all'accesso	0	
Misure Idonee	/	Esistenza di una lista di requisiti standard per il software da installare	0	
Misure Idonee	/	Installazione solo di software licenziato	50	
Misure Idonee	/	Divieto di software non approvato	0	
Misure Idonee	/	Controlli sul tipo di software installato al fine di rilevare quelli non approvati	50	

Misure Idonee	/	Linee di alimentazione elettrica e di comunicazione interrate o alternativamente protette in modo adeguato	100
Misure Idonee	/	Procedure per la comunicazione dei cambiamenti organizzativi interni (es. turnover)	0

Tabella 7 Misure di sicurezza minime e idonee relative ai trattamenti con l'ausilio di strumenti elettronici non direttamente associate alle banche dati

4.2. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Nelle tabelle che seguono è riportato il grado di copertura dell' Ente in relazione alle misure di sicurezza associabili (Tabella 8) e non associabili (Tabella 9) alle banche dati, relativamente ai trattamenti svolti senza l'ausilio di strumenti elettronici.

In particolare ogni tabella contiene i seguenti campi:

- **Riferimento al T.U.:** contiene il riferimento all'articolo del Disciplinare Tecnico del Testo Unico nel quale sono esplicitate le misure di sicurezza previste dalla Legge;
- **Misure di sicurezza:** contiene la descrizione delle misure minime di sicurezza contenute nel corrispondente articolo del Disciplinare Tecnico del T.U. e la descrizione delle misure idonee per la protezione delle aree e dei locali;
- **Grado di copertura:**
  - per le misure di sicurezza associate alle banche dati: il grado di copertura equivale alla completa adozione (100%), parziale adozione (50%) o meno (0%) della misura di sicurezza nell'Ente;
  - per le misure di sicurezza non associabili alle banche dati: il grado di copertura equivale alla completa adozione (100%), parziale adozione (50%) o meno (0%) della misura di sicurezza nell'Ente;
  - nel caso in cui non esistano le condizioni per l'applicabilità della misura di sicurezza sarà riportata la dicitura "N.a.", cioè non applicabile.

4.2.1. MISURE DI SICUREZZA ASSOCIATE ALLE BANCHE DATI

Tipologia di Misura	Rif. Testo Unico	Misure "Minime" di sicurezza - Trattamenti effettuati senza l'ausilio di strumenti elettronici	Misura già in essere	
Cartacea	Disciplinare Tecnico n°29	Accesso controllato agli archivi contenenti dati sensibili o giudiziari	70	
Cartacea	Disciplinare Tecnico n°29	Accesso dopo l'orario di chiusura agli archivi contenenti dati personali o sensibili	si	
Cartacea	Disciplinare Tecnico n°29	Le persone ammesse, agli archivi contenenti dati sensibili e giudiziari, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate		100
Cartacea	Disciplinare Tecnico n°29	Quando gli archivi, contenenti dati sensibili e giudiziari, non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate		na

	Riferimento Testo Unico	Misure "Idonee" di sicurezza - Trattamenti effettuati senza l'ausilio di strumenti elettronici	
Idonea	/	Esiste un servizio di vigilanza	100
Idonea	/	Esiste un servizio di videosorveglianza	0
Idonea	/	Sistemi di allarme e/o antintrusione	10
Idonea	/	Sistemi antincendio	50
Idonea	/	Sui sistemi antincendio sono effettuati controlli periodici	100
Idonea	/	Sistemi di rilevazione fumi	50
Idonea	/	Impianto di antiallagamento	0
Idonea	/	Chiusura a chiave dei locali o contenitori contenenti i dati cartacei in assenza di personale	50
Idonea	/	Nomina di custodi delle chiavi dei locali in cui si trovano gli archivi cartacei	0

Tabella 8 Misure di sicurezza minime e idonee relative ai trattamenti senza l'ausilio di strumenti elettronici direttamente associate alle banche dati

4.2.2. MISURE DI SICUREZZA NON ASSOCIATE ALLE BANCHE DATI

Tipologia di Misura	Rir. Testo Unico	Misure "Minime" di sicurezza Trattamenti effettuati senza l'ausilio di strumenti elettronici	Misura già in essere
Cartacea	Disciplinare Tecnico n°27	Esistenza di specifiche istruzioni scritte rilasciate agli incaricati finalizzate al controllo e alla custodia degli atti e dei documenti contenenti dati personali, per l'intero ciclo necessario allo svolgimento dei propri compiti	100
Cartacea	Disciplinare Tecnico n°27	Aggiornamento periodico (almeno annuale) della lista degli incaricati e del relativo ambito del trattamento dei dati personali	100
Cartacea	Disciplinare Tecnico n°28	Gli Incaricati del trattamento cui sono affidati di atti e documenti contenenti dati sensibili o giudiziari prestano un costante presidio sugli stessi (i medesimi atti e documenti sono controllati e custoditi dagli stessi incaricati fino alla restituzione in modo che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate)	50
	Riferimento Testo Unico	Misure "Idonee" di sicurezza Trattamenti effettuati senza l'ausilio di strumenti elettronici	
Idonea	/	Accesso agli edifici controllato da un servizio di guardia/portineria	10
Idonea	/	Utilizzo di un distruggi documenti	0
Idonea	/	Fotocopiatrici localizzate in locali idonei	100
Idonea	/	Procedure per la comunicazione dei cambiamenti organizzativi interni (es. turn-over)	100

Tabella 9 Misure di sicurezza / adempimenti relativi ai trattamenti senza l'ausilio di strumenti elettronici non associati direttamente alle banche dati

5. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

5.1. LA METODOLOGIA ADOTTATA

L'analisi dei rischi si è svolta in tre fasi distinte:

- individuazione e analisi dei rischi;
- valutazione dei rischi al fine di evidenziare i punti di forza e di debolezza dell' Ente in tema di protezione dei dati personali;
- identificazione degli interventi di adeguamento in funzione delle criticità rilevate.

Individuazione e analisi dei rischi

L'individuazione dei rischi è stata fatta con un sistema cosiddetto "a protezione zero", valutando astrattamente i potenziali rischi che incombono sui dati, a prescindere dalle misure già adottate dall' Ente. In particolare tali rischi sono stati individuati sulla base dei seguenti requisiti:

- **la riservatezza,** ossia la prevenzione dell'utilizzo indebito di informazioni riservate contenute nelle banche dati;
- **l'integrità,** ovvero la prevenzione della alterazione o manipolazione indebita dei dati e delle informazioni contenute nelle banche dati.
- **la disponibilità,** ovvero garanzia dell'accesso controllato dei dati e delle informazioni contenute nelle banche dati.

Valutazione dei rischi

Una volta individuati i rischi si è proceduto alla valutazione degli stessi.
La valutazione è finalizzata al calcolo quantitativo del livello di rischio associato ad ognuno dei rischi individuati.
La metodologia utilizzata per la valutazione dei rischi prende in considerazione il grado di copertura della struttura rispetto:

- alle misure minime ritenute dal legislatore necessarie e sufficienti ad escludere i rischi particolarmente gravi per i dati sottoposti a trattamento in quanto esiste, alla data di stesura del presente documento, un intervallo temporale per l'adeguamento obbligatorio di talune misure (entro il 31 marzo 2006);
- alle misure cosiddette idonee, rivolte a ridurre al minimo tutti gli altri rischi che possono incombere sui dati personali.

Le misure di sicurezza idonee considerate nella valutazione dei rischi sono state scelte in base a quattro elementi specificamente indicati nel Testo Unico:

- progresso tecnico;
- natura dei dati;
- caratteristiche del trattamento;

- altri rischi non specificamente indicati nel Testo Unico (ad es. indisponibilità dei dati, inadempienza a specifiche disposizioni di legge, ecc.).

La valutazione fornita non deve essere considerata "assoluta" ma solo relativa alla metodologia adottata. Infatti, il risultato ottenuto si riferisce ad un numero "limitato" di misure di sicurezza idonee. Questo significa che un livello di rischio è alto o basso solo se confrontato con gli altri livelli di rischio calcolati.

Individuazione degli interventi di adeguamento

L'obiettivo è di individuare gli interventi più opportuni in funzione delle criticità rilevate in fase di valutazione, al fine di ridurre i rischi che incombono sui dati all'interno dell' Ente.
Gli interventi di adeguamento riguardano:

- le nuove misure di sicurezza minime che devono essere adottate entro il 31 dicembre 2005 (rif. Dlg. giugno 2004), anche se, nel caso in cui il Titolare dei trattamenti di dati personali e/o sensibili, gestiti con strumenti elettronici, non sia in grado di adottare completamente o in parte le misure minime di sicurezza per obiettive ragioni tecniche entro tale termine, ha la possibilità di chiedere, con documento a data certa, un'ulteriore proroga al 31 marzo del 2006;
- le misure di sicurezza idonee in funzione del livello di riduzione del rischio che generano.

5.2. INDIVIDUAZIONE DEI RISCHI

I rischi individuati sulla base dei requisiti precedentemente descritti sono:

- **Riservatezza**
  Salvaguardare la riservatezza significa eliminare o quanto meno ridurre a livelli accettabili i rischi di:

  1. accesso non autorizzato, ossia il rischio che un soggetto possa "utilizzare" dei dati e delle informazioni senza autorizzazione;
     L'accesso non autorizzato potrebbe portare a:
     - distruzione o perdita
     - compromissione dell'integrità
     - alterazione
     - copia abusiva
     - furto
     - divulgazione

     e può essere frutto di un attacco deliberato da parte di personale dipendente o di terzi; può avvenire dall'interno o dall'esterno durante il normale orario di lavoro per i dipendenti o al di fuori di questo nel caso di terzi presenti all'interno dei locali dell' Ente con regolare autorizzazione.

  2. trattamento di dati non consentito o non conforme alle finalità del trattamento

Il trattamento non consentito o non conforme alle finalità della raccolta potrebbe portare a:

- distruzione o perdita
- compromissione dell'integrità
- alterazione

e può essere frutto di un attacco deliberato da parte di personale dipendente o di terzi; può avvenire dall'interno o dall'esterno durante il normale orario di lavoro per i dipendenti o al di fuori di questo nel caso di terzi presenti all'interno dei locali dell' Ente con regolare autorizzazione.

- **Integrità**

Garantire l'integrità significa eliminare o ridurre a livelli accettabili il rischio di:

3. perdita o distruzione parziale dei dati a seguito di interventi da parte di soggetti non autorizzati o di eventi straordinari come allagamenti, incendi, furti, ecc...
   Il rischio di perdita o di distruzione, totale o parziale, può essere determinato da:
   - incendio
   - avaria, danneggiamento, mancanza di energia elettrica o infezione da virus per quanto riguarda gli elaboratori (server e client) che hanno dati residenti sui propri sottosistemi dischi
   - anomalia di funzionamento del SW di base (sistemi operativi, data base, ecc.)
   - anomalia di funzionamento del SW applicativo
   - accesso non autorizzato al sistema operativo o al SW applicativo
   - accesso non autorizzato ai locali dove si esegue il trattamento (CED, archivi cartacei, ecc.)
   - furto, danneggiamento, alterazione o copia abusiva dei supporti magnetici di back up e può essere accidentale, dovuta a guasto di apparecchiature o ad errore umano, piuttosto che frutto di un attacco deliberato da parte di personale dipendente o di terzi; può avvenire dall'interno o dall'esterno durante il normale orario per i dipendenti o al di fuori di questo nel caso di terzi presenti all'interno dei locali dell' Ente con regolare autorizzazione.
   -

- **Disponibilità**

Garantire la disponibilità equivale a prevenire il rischio di:

4. indisponibilità dei dati, ossia l'impossibilità di accesso a dati o risorse necessarie allo svolgimento di una attività lecita di trattamento dovuto o all'assenza prolungata/ impedimento di un incaricato o alla perdita/distruzione dei dati a seguito di interventi da parte di soggetti non autorizzati o di eventi straordinari come allagamenti, incendi, furti, etc.

garantendo la completezza e la correttezza dei dati da trattare.

Accanto alle categorie di rischio indicate, che possono essere "abbattute" attraverso l'adozione di misure di sicurezza contenute nel Testo Unico, è stata prevista un'ulteriore categoria di rischio:

5. inadempienze a specifiche disposizioni di legge

per tenere conto di altri obblighi di legge la cui inosservanza può provocare specifiche sanzioni penali, amministrative e civili.

Ad ognuno dei rischi individuati sono state associate le misure di sicurezza (minime e idonee) che, se adottate, consentono di ridurre al minimo il relativo rischio.

5.3. VALUTAZIONE DEI RISCHI

La valutazione del livello di rischio totale è rappresentata in forma tabellare e contiene i seguenti campi nell'ordine con cui sono descritti:

- **Riferimento al T.U.:** contiene il riferimento all'articolo del Disciplinare Tecnico del Testo Unico nel quale sono esplicitate le misure di sicurezza previste dalla Legge;
- **ipologia di misura di sicurezza:** indica se la misura è minima o idonea;
- **Misure di sicurezza associate ai rischi**: indicano le misure di sicurezza (minime e idonee) che, se adottate dal Titolare, consentono di ridurre al minimo il relativo rischio; le misure di sicurezza evidenziate con il colore verde indicano le misure non associabili direttamente alle banche dati;
- **Livello di rischio totale**: il livello di rischio totale è la media dei livelli di rischio per singola misura di sicurezza.

  La determinazione del livello di rischio per singola misura di sicurezza dipende dall'associazione o meno della stessa alle banche dati presenti nell'Ente. In particolare nel caso di:

  - misura di sicurezza associabile alle banche dati: il livello di rischio per singola misura di sicurezza è uguale al rischio medio ponderato calcolato sulla base della copertura della misura di sicurezza per ogni trattamento e della "criticità" della banca dati stessa, in termini di natura dei dati contenuti (dati comuni o dati sensibili/giudiziari);
  - misura di sicurezza non associabile alle banche dati: il livello di rischio per singola misura di sicurezza è valutato in base all'adeguamento o meno dell' Ente alla misura di sicurezza stessa. Per convenzione, l'adeguamento o meno alla misura è valutato rispettivamente con un livello di rischio pari a 0 e a 1. Adeguamenti parziali alla misura sono valutati con un livello di rischio pari a 0,5.

  Sono stati individuati i seguenti tre livelli di rischio totale:

  - Rischio basso: tra 0 e 0,6
  - Rischio medio: tra 0,7 e 1,3
  - Rischio alto: tra 1,4 e 2

Come già detto, il livello di rischio calcolato non ha valore assoluto ma è utile per essere confrontato con gli altri livelli di rischio ottenuti, dello stesso presidio, e per monitorare gli interventi migliorativi che saranno intrapresi.

5.3.1. ACCESSO NON AUTORIZZATO

Rif.	Tipologia misura di sicurezza	Descrizione Misura di Sicurezza	Rishio per Misura
Disciplinare Tecnico n° 2	M	Assegnazione ad ogni incaricato di una o più credenziali di autenticazione che consenta il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti	1,5
Disciplinare Tecnico n° 2	M	Credenziali di autenticazione conosciute solo dall'incaricato e ad esso univocamente correlate	1,5
Disciplinare Tecnico n° 7	M	Disattivazione delle credenziali di autenticazione non utilizzate da almeno 6 mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (es utilizzate dagli amministratori di sistema)	1,5
Disciplinare Tecnico n° 8	M	Disattivazione delle credenziali nel caso in cui l'incaricato perda la qualità (ruolo/compito) per l'accesso ai dati personali	1,5
Disciplinare Tecnico n° 5	M	Parola chiave, quando prevista dal sistema di autenticazione, composta da almeno 8 caratteri	2
Disciplinare Tecnico n° 5	M	Parola chiave composta da un numero di caratteri pari al massimo consentito (nel caso in cui lo strumento elettronico non permetta la creazione di password di 8 caratteri)	2
Disciplinare Tecnico n° 5	M	Modifica della parola chiave da parte degli Incaricati al primo utilizzo	1
Disciplinare Tecnico n° 5	M	Modifica della parola chiave, nel caso di trattamenti di dati comuni, da parte degli Incaricati almeno ogni 6 mesi	2
Disciplinare Tecnico n° 5	M	Modifica della parola chiave, nel caso di trattamento di dati sensibili e di dati giudiziari, almeno ogni 3 mesi	2
Disciplinare Tecnico n° 4	M	Esistenza di specifiche istruzioni scritte rilasciate agli incaricati, in cui è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale	0

Disciplinare Tecnico n° 5	M	Formalizzazione del divieto di comporre la parola chiave con riferimenti agevolmente riconducibili all'incaricato (es. nome, data di nascita, nomi di familiari)	0
Disciplinare Tecnico n°6	M	Codice per l'identificazione, laddove usato, non è assegnato ad altri incaricati, neppure in tempi diversi	1,5
Disciplinare Tecnico n° 9	M	Esistenza di specifiche istruzioni scritte rilasciate agli incaricati, in cui è prescritto di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento	0
Disciplinare Tecnico n° 10	M	Definizione di procedure che disciplinano le modalità operative per informare tempestivamente l'incaricato circa l'utilizzo della propria credenziale di autenticazione	0
Disciplinare Tecnico n° 12	M	Sistema di autorizzazione nel caso in cui l'incaricato ha più profili di autorizzazione con ambiti diversi	0
Disciplinare Tecnico n° 13	M	Individuazione e configurazione prima dell'inizio del trattamento dei profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati	1
Disciplinare Tecnico n° 14	M	Verifica periodica (almeno annuale) della sussistenza delle condizioni per la conservazione dei profili di autorizzazione	1,5
Disciplinare Tecnico n°16	M	Implementazione di strumenti elettronici per garantire la protezione dei dati personali contro il rischio di intrusione (Firewall) e dell'azione di virus o software dannosi (Antivirus)	0
Disciplinare Tecnico n°16	M	Aggiornamento di tali strumenti con cadenza almeno semestrale	0
/	I	Esiste un servizio di vigilanza	1
/	I	Esiste un servizio di videosorveglianza	1
/	I	Sistemi di allarme e/o antintrusione	1
/	I	Locale chiuso a chiave in assenza di personale	0
/	I	Nomina di custodi delle chiavi dei locali in cui si trovano gli strumenti elettronici	0
/	I	Log delle attività svolte dagli incaricati mediante un'applicazione	1
/	I	Presenza di una persona che controlla periodicamente i log delle applicazioni	1
/	I	Adozione di un software per la gestione delle utenze	0,5
/	I	Esistenza di documentazione aggiornata sulle configurazioni dei db/server/applicativi	1

/	I	Effettuazione di configurazioni di sicurezza per la protezione del sistema e dei dati ivi contenuti (ad es. attivo il File System NTFS, effettuato hardening del sistema operativo, ecc.)	0
/	I	Accesso agli edifici controllato da un servizio di guardia/portineria	1
/	I	Dispositivi per la sospensione temporanea o definitiva (previo intervento dell'amministratore di sistema) dell'accesso, dopo la digitazione errata per n volte della password	1
/	I	Procedure per la comunicazione dei cambiamenti organizzativi interni (es. turnover)	1
LIVELLO DI RISCHIO TOTALE			**0,89**

Tabella 10 Misure di sicurezza associate ai rischi di accesso non autorizzato (trattamenti con l'ausilio di strumenti elettronici)

Rif.	Tipologia misura di sicurezza	Descrizione Misura di Sicurezza	Rishio per Misura
Disciplinare Tecnico n°28	M	Gli Incaricati del trattamento cui sono affidati di atti e documenti contenenti dati sensibili o giudiziari prestano un costante presidio sugli stessi (i medesimi atti e documenti sono controllati e custoditi dagli stessi incaricati fino alla restituzione in modo che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate)	0,5
Disciplinare Tecnico n°29	M	Accesso controllato (verifica dell'identità della persona) agli archivi contenenti dati sensibili o giudiziari	1,3
Disciplinare Tecnico n°29	M	Le persone ammesse, agli archivi contenenti dati sensibili e giudiziari, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate	0
/	I	Esiste un servizio di vigilanza	0
/	I	Esiste un servizio di videosorveglianza	1
/	I	Sistemi di allarme e/o antintrusione	0,9
/	I	Chiusura a chiave dei locali o contenitori contenenti i dati cartacei in assenza di personale	0,5
/	I	Nomina di custodi delle chiavi dei locali in cui si trovano gli archivi cartacei	1
/	I	Accesso agli edifici controllato da un servizio di guardia/portineria	0,9

/	I	Procedure per la comunicazione dei cambiamenti organizzativi interni (es. turnover)	0
LIVELLO DI RISCHIO TOTALE			**0,61**

Tabella 11 Misure di sicurezza associate ai rischi di accesso non autorizzato (trattamenti senza l'ausilio di strumenti elettronici)

5.3.2. TRATTAMENTO NON CONSENTITO O NON CONFORME ALLE FINALITÀ DELLA RACCOLTA

Rif.	Tipologia misura di sicurezza	Descrizione Misura di Sicurezza	Rishio per Misura
Disciplinare Tecnico n° 15	M	Aggiornamento periodico (almeno annualmente) della lista degli incaricati e degli addetti alla gestione/manutenzione degli strumenti elettronici e del relativo ambito del trattamento dei dati personali	1
Disciplinare Tecnico n°21	M	Esistenza di istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati (sensibili e giudiziari) al fine di evitare accessi non autorizzati e trattamenti non consentiti	0
Disciplinare Tecnico n°22	M	I supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, sono distrutti o resi inutilizzabili	1
Disciplinare Tecnico n°22	M	I supporti rimovibili contenenti dati sensibili o giudiziari vengono riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, esclusivamente nell'ipotesi in cui le informazioni non siano intelligibili e tecnicamente in alcun modo recuperabili	1
/	I	Predisposizione di linee e/o numeri dedicati per la trasmissione di dati sensibili, con limitazioni all'accesso	1
LIVELLO DI RISCHIO TOTALE			**0,80**

Tabella 12 Misure di sicurezza associate ai rischi di trattamento non consentito o non conforme alle finalità del trattamento (trattamenti con l'ausilio di strumenti elettronici)

Rif.	Tipologia misura di sicurezza	Descrizione Misura di Sicurezza	Rishio per Misura
Disciplinare Tecnico n°27	M	Esistenza di specifiche istruzioni scritte rilasciate agli incaricati finalizzate al controllo e alla custodia degli atti e dei documenti contenenti dati personali, per l'intero ciclo necessario allo svolgimento dei propri compiti	0
Disciplinare Tecnico n°27	M	Aggiornamento periodico (almeno annuale) della lista degli incaricati e del relativo ambito del trattamento dei dati personali	0
/	I	Utilizzo di un distruggi documenti	1
/	I	Fotocopiatrici localizzate in locali idonei	0
LIVELLO DI RISCHIO TOTALE			**0,25**

Tabella 13 Misure di sicurezza associate ai rischi di trattamento non consentito o non conforme alle finalità del trattamento (trattamenti senza l'ausilio di strumenti elettronici)

5.3.3. PERDITA O DISTRUZIONE DEI DATI

Rif.	Tipologia misura di sicurezza	Descrizione Misura di Sicurezza	Rishio per Misura
/	I	Sistemi antincendio	0,5
/	I	Sui sistemi antincendio sono effettuati controlli periodici	0
/	I	Sistemi di rilevazione fumi	0,5
/	I	Impianto di antiallagamento	1
LIVELLO DI RISCHIO TOTALE			**0,50**

Tabella 14 Misure di sicurezza associate ai rischi di perdita o distruzione (trattamenti con l'ausilio di strumenti elettronici)

Rif.	Tipologia misura di sicurezza	Descrizione Misura di Sicurezza	Rischio per Misura
Disciplinare Tecnico n°17	M	Aggiornamento dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti (es. SERVICE PACK E PATCHES) almeno annuale	0
Disciplinare Tecnico n°17	M	Aggiornamento di questi sw, in caso di trattamento di dati sensibili o giudiziari, almeno semestrale	0
Disciplinare Tecnico n° 18	M	Esistenza di istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale	0
Disciplinare Tecnico n°23	M	Sono state adottate idonee misure e specifiche procedure per garantire il ripristino dell'accesso ai dati (sensibili e giudiziari) in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati (max 7 gg)	1
/	I	Sistemi antincendio	0,5
/	I	Effettuazione di controlli periodici sui sistemi antincendio	0,5
/	I	Sistemi di rilevazione fumi	0
/	I	Gruppi di continuità elettrica	0
/	I	Impianto di antiallagamento	1
/	I	Apparecchiature installate in aree chiuse o protette (server gateway, router)	0,5
/	I	Dispositivi per la limitazione dell'accesso a particolari siti web potenzialmente pericolosi	1
/	I	Installazione solo di software licenziato	0,5
/	I	Divieto di software non approvato	1
/	I	Controlli sul tipo di software installato al fine di rilevare quelli non approvati	0,5
/	I	Linee di alimentazione elettrica e di comunicazione interrate o alternativamente protette in modo adeguato	0
LIVELLO DI RISCHIO TOTALE			**0,43**

Tabella 15 Misure di sicurezza associate ai rischi di perdita o distruzione (trattamenti senza l'ausilio di strumenti elettronici)

5.3.4. INDISPONIBILITÀ DEI DATI

Rif.	Tipologia misura di sicurezza	Descrizione Misura di Sicurezza	Rishio per Misura
Disciplinare Tecnico n° 10	M	Esistenza di disposizioni scritte che individuano le modalità con le quali il Titolare può assicurare, in caso di necessità operativa, la disponibilità dei dati o degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato	0
Disciplinare Tecnico n° 10	M	Individuazione per iscritto dei soggetti incaricati della custodia delle credenziali di autenticazione nel caso in cui sia tecnicamente impossibile garantire l'accesso ai dati	0
Disciplinare Tecnico n° 10	M	Formalizzazione di procedure che disciplinino la custodia delle copie delle credenziali garantendo la massima segretezza	0
/	I	Verifiche della leggibilità dei supporti di backup	1
/	I	Custodia dei supporti (es. di backup) in contenitori ignifughi	1
/	I	Custodia dei supporti di backup in luoghi diversi da quelli in cui si trovano i computer in cui sono memorizzati i dati	1
/	I	Effettuazione periodica di test di verifica delle vulnerabilità del sistema server su cui risiede la banca dati	1
/	I	Aggiornamento tempestivo delle vulnerabilità del sistema operativo	0
LIVELLO DI RISCHIO TOTALE			**0,50**

Tabella 16 Misure di sicurezza associate ai rischi di indisponibilità dei dati (trattamenti con l'ausilio di strumenti elettronici)

5.3.5. INADEMPIENZE A SPECIFICHE DISPOSIZIONI DI LEGGE

Rif.	Tipologia misura di sicurezza	Descrizione Misura di Sicurezza	Rishio per Misura
Disciplinare Tecnico n°19	M	Redazione del Documento Programmatico sulla Sicurezza nell'ipotesi di trattamenti di dati sensibili e giudiziari	0

Disciplinare Tecnico n°19	M	Aggiornamento del documento entro il 31 marzo di ogni anno	0
Disciplinare Tecnico n°19	M	Analisi dei rischi	0
Disciplinare Tecnico n°19	M	Piano di formazione per gli incaricati	0
Disciplinare Tecnico n°19	M	Adozione di criteri per garantire l'adozione di misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare (OUTSOURCING)	0
Disciplinare Tecnico n°25	M	Qualora ci si avvalga di soggetti esterni alla propria struttura per adottare misure minime di sicurezza si richiede all'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare	0,5
Disciplinare Tecnico n°26	M	Nella relazione accompagnatoria del bilancio (se dovuta), il titolare riferisce l'avvenuta redazione o aggiornamento del Documento Programmatico sulla Sicurezza	1
/	I	Esistenza di una lista di requisiti standard per il software da installare	1
LIVELLO DI RISCHIO TOTALE			**0,31**

Tabella 17 Misure di sicurezza associate ai rischi di inadempienze a specifici obblighi di legge (trattamenti senza l'ausilio di strumenti elettronici)

5.4. INDIVIDUAZIONE DEGLI INTERVENTI DI ADEGUAMENTO

A fronte dell'analisi dei rischi eseguita, della quale sono sintetizzati nella seguente tabella i risultati, si riporta una proposta di piano di adeguamento:

Rischi	Trattamento con l'ausilio di strumenti elettronici	Trattamento senza l'ausilio di strumenti elettronici	Indipendente dalla modalità di trattamento
Accesso non autorizzato	**0,89**	**0,61**	**N.A.**
Trattamento non consentito o non conforme alla finalità della raccolta	**0,80**	**0,25**	**N.A.**
Perdita e distruzione	**0,43**	**0,50**	**N.A.**
Indisponibilità dei dati	**0,50**	**N.A.**	**N.A.**
Inadempienze a specifiche disposizioni di legge	**N.A.**	**N.A.**	**0,31**

Tabella 18 Sintesi della valutazione dei rischi per tipologia

Legenda:

Rischio basso tra 0 e 0,6	**Rischio medio** tra 0,7 e 1,3	Rischio alto tra 1,4 e 2	Rischio non applicabile –

In particolare la priorità degli interventi di adeguamento è legata:

- alle scadenze di legge per le misure minime di sicurezza
- al livello del rischio ottenuto:
  - livello di rischio medio/alto: interventi di adeguamento prioritari
  - livello di rischio basso: interventi di adeguamento secondari

Il piano di adeguamento è rappresentato in forma tabellare e contiene i seguenti campi:

- **Rischio:** contiene il tipo di rischio che può essere ridotto con gli interventi di adeguamento proposti;

- **Modalità di trattamento:** indica se il trattamento è effettuato con o senza l'ausilio di strumenti elettronici;
- **ipologia di misura di sicurezza:** indica la tipologia della misura di sicurezza che deve essere adottata dal presidio ed in particolare;

Codice tipologia	Descrizione tipologia
M	Misura minima di sicurezza coma da Disciplinare Tecnico del D.lgs. n.196/03
I	Misura idonea di sicurezza

- **Attività**: indica le misure di sicurezza (minime e idonee) che, devono essere adottate dal Titolare per ridurre il relativo rischio.
  La nuova scadenza per l'applicazione delle misure minime di sicurezza è il 31 dicembre 2005 (rif. Dlg. giugno 2004), ma nel caso in cui il Titolare dei trattamenti di dati personali e/o sensibili, gestiti con strumenti elettronici, non sia in grado di adottare completamente o in parte le misure minime di sicurezza per obiettive ragioni tecniche entro tale termine, ha la possibilità di chiedere, con documento a data certa, un'ulteriore proroga (31 marzo del 2006);
- **Strutture o persone addette all'adozione:** Indica la figura/struttura aziendale principalmente coinvolta nell'attività di adeguamento;
- **empi:** contiene una tempificazione degli interventi di adeguamento proposti;
- **Note**

5.4.1. INTERVENTI DI ADEGUAMENTO PRIORITARI

Rischio	Modalità di Trattamento	Tipologia misura	Attività di Adeguamento	Struttura o persone addette all'adozione	Tempi previsti
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Provvedere ad assegnare agli Incaricati User-Id e Pw	CED	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Disabilitare le password e user-id comuni a più incaricati ed assegnarne di personali	CED	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Configurare i sistemi di autenticazione impostando la disabilitazione delle credenziali dopo 6 msei di inutilizzo	CED	Scadenze di legge

Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Predisporre una procedura per la comunicazione dei cambiamenti organizzativi interni (turnover), al fine di tenere costantemente aggiornati i profili di autorizzazione e relativi codici identificativi e password	Titolare/Referente Privacy/Ufficio Personale	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Provvedere alla composizione della parola chiave di almeno 8 caratteri	CED	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Provvedere alla composizione della parola chiave di un numero di caratteri pari al massimo consentito dal sistema	CED	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Predisporre la modifica della parola chiave, da parte degli Incaricati, almeno ogni 6 mesi, nel caso di trattamenti di dati comuni, e almeno ogni 3 mesi, nel caso di trattamenti di dati sensibili	CED/Incaricati	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Predisporre la modifica della parola chiave, da parte degli Incaricati, almeno ogni 6 mesi, nel caso di trattamenti di dati comuni, e almeno ogni 3 mesi, nel caso di trattamenti di dati sensibili	CED/Incaricati	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Utilizzare esclusivamente user-id originali	CED	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Verificare periodicamente (almeno annualmente) la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	Responsabili del trattamento	Ogni anno

Tabella 19 Piano di adeguamento degli interventi prioritari

5.4.2. INTERVENTI DI ADEGUAMENTO SECONDARI

Rischio	Modalità di Trattamento	Tipologia misura	Attività di Adeguamento	Struttura o persone addette all'adozione	Tempi previsti
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Predisporre la modifica della parola chiave da parte degli Incaricati al primo utilizzo	CED/Incaricati	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	M	Predisporre dei sistemi di autorizzazione nel caso in cui l'incaricato ha più profili di autorizzazione con ambiti diversi	Responsabili del trattamento/CED	Scadenze di legge
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Istituire un servizio di vigilanza	Titolare	
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Predisporre un sistema di videosorveglianza	Titolare	
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Predisporre un sistema di allarme nel locale CED		
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Dotarsi di un'applicazione che permetta di rilevare il Log delle attività svolte dagli incaricati al fine di controllare gli accessi ai dati	Responsabile del trattamento IT	
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Predisporre il controllo dei log da parte di personale addetto	Incaricati alla gestione e manutenzion IT/Responsabile del trattamento IT	
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Aggiornare la documentazione sulle configurazioni dei db/server/applicativi	CED	
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Istituire un servizio di portierato	Titolare	
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Predisporre dei dispositivi per la sospensione temporanea o definitiva (previo intervento dell'amministratore di sistema) dell'accesso, dopo la digitazione errata per n volte della password	CED	

Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Predisporre una procedura per la comunicazione dei cambiamenti organizzativi interni (turnover), al fine di tenere costantemente aggiornati i profili di autorizzazione e relativi codici identificativi e password	Titolare/Referente Privacy/Ufficio Personale	
Accesso non autorizzato	Trattamento senza l'ausilio di strumenti elettronici	M	Predisporre il controllo degli accessi agli archivi contenenti dati sensibili/giudiziari	Responsabili	Scadenze di legge
Accesso non autorizzato	Trattamento senza l'ausilio di strumenti elettronici	I	Predisporre un servizio di videosorveglianza	Titolare	
Accesso non autorizzato	Trattamento senza l'ausilio di strumenti elettronici	I	Predisporre un sistema antintrusione	Titolare	
Accesso non autorizzato	Trattamento senza l'ausilio di strumenti elettronici	I	Nominare i custodi delle chiavi dei locali in cui si trovano gli archivi cartacei	Titolare/Responsabili	
Accesso non autorizzato	Trattamento senza l'ausilio di strumenti elettronici	I	Predisporre un servizio di portineria	Titolare	
Inadempienza a specifiche disposizioni di legge	Indipendente dalla modalità di trattamento	M	Provvedere a riferire dell'avvenuta redazione del DPS nella relazione accompagnatoria al bilancio di esercizio	Titolare	Ogni anno
Inadempienza a specifiche disposizioni di legge	Indipendente dalla modalità di trattamento	I	Stilare una lista di requisiti standard per il software da installare	CED	
Indisponibilità dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Provvedere a verificare la leggibilità delle copie di backup	CED	
Indisponibilità dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Custodire i supporti (es. di backup) in contenitori ignifughi	CED	
Indisponibilità dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Custodire i supporti di backup in luoghi diversi da quelli in cui si trovano i computer in cui sono memorizzati i dati	CED	
Indisponibilità dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Effettuare periodicamenti i test di verifica delle vulnerabilità del sistema server su cui risiede la banca dati	CED	

Perdita e distruzione dei dati	Trattamento con l'ausilio di strumenti elettronici	M	Predisporre un piano di disaster recovery che consenta il ripristino all'accesso adi dati o agli strumenti elettronici in caso di danneggiamento in tempi certi, di al massimo 7 gg	CED	Scadenze di legge
Perdita e distruzione dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Impianto di antiallagamento per la sala CED	CED	
Perdita e distruzione dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Adottare dispositivi tecnici per la limitazione dell'accesso a particolari siti web potenzialmente pericolosi	CED	
Perdita e distruzione dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Vietare l'installazione di SW non approvato	Titolare/Responsabile del trattamento IT	
Perdita e distruzione dei dati	Trattamento senza l'ausilio di strumenti elettronici	I	Impianto di antiallagamento degli archivi interni alla struttura contenenti banche dati cartacee	Titolare/Responsabili	
Trattamento non consentito	Trattamento con l'ausilio di strumenti elettronici	M	Provvedere all'aggiornamento annuale della lista degli incaricati e addettialla manutenzione degli strumenti elettronici e del relativo ambito del trattamento	Responsabili del trattamento	Ogni anno
Trattamento non consentito	Trattamento con l'ausilio di strumenti elettronici	M	Provvedere alla distruzione dei supporti removibili contenteti dati sensibili non più utilizzati	Incaricati	Scadenze di legge
Trattamento non consentito	Trattamento con l'ausilio di strumenti elettronici	M	Permettere il riutilizzo dei supporti removibili contenenti dati sensibli ad altre persone solo se i dati precedentemente memorizzati sono stati non intellegibili e irrecuperabili	Incaricati	Scadenze di legge
Trattamento non consentito	Trattamento con l'ausilio di strumenti elettronici	I	Predisporre linee e/o numeri dedicati per la trasmissione di dati sensibili, con limitazioni all'accesso utilizzo	CED	Scadenze di legge
Trattamento non consentito	Trattamento senza l'ausilio di strumenti elettronici	I	Utilizzare un distruggi documenti	Titolare/Responsabili	
Accesso non autorizzato	Trattamento con l'ausilio di strumenti elettronici	I	Adottare un software per la gestione in automatico delle utenze	Responsabilie del trattamento IT	
Accesso non autorizzato	Trattamento senza l'ausilio di strumenti elettronici	M	Formalizzazione di procedure che prevedano il costante presidio della documentazione sensibile e giudiziara ad opera degli incaricati durante le operazioni del trattamento	Titolare/Responsabili	Scadenze di legge

Accesso non autorizzato	Trattamento senza l'ausilio di strumenti elettronici	I	In assenza di personale, provvedere a chiudere a chiave i locali o i contenitori contenenti i dati cartacei particolarmente sensibili (dati sensibili e/o giudiziari)	Incaricati	
Inadempienza a specifiche disposizioni di legge	Indipendente dalla modalità di trattamento	M	Qualora ci si avvalga di soggetti esterni alla propria struttura per adottare misure minime di sicurezza richiedere all'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare	CED/Responsabili	Ad ogni installazione
Perdita e distruzione dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Predisporre un sistema antincendio per la sala CED	CED	
Perdita e distruzione dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Effettuare controlli periodici sul sistema antincendio per la sala CED	CED	
Perdita e distruzione dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Installare la sala macchine CED in luoghi chiusi e protetti	Responsabile trattamento IT	
Perdita e distruzione dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Installare solamente software licenziato	CED	
Perdita e distruzione dei dati	Trattamento con l'ausilio di strumenti elettronici	I	Effettuare dei controlli sul tipo di software installato al fine di rilevare quelli non approvati	CED	
Perdita e distruzione dei dati	Trattamento senza l'ausilio di strumenti elettronici	I	Predisporre un sistema antincendio	Titolare/Responsabili	
Perdita e distruzione dei dati	Trattamento senza l'ausilio di strumenti elettronici	I	Predisporre un sistema di rilevazione di fumi	Titolare/Responsabili	

Tabella 20 Piano di adeguamento degli interventi secondari

6. CRITERI E MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI

Si veda "Istra_BN01_01", allegato al presente documento e parte integrante del Documento Programmatico sulla Sicurezza.

7. ELABORAZIONE DEL PIANO DI FORMAZIONE

Per rendere noti i rischi individuati e le modalità per prevenire i relativi danni, la Provincia di Benevento ha varato un piano di formazione. In particolare, per tutti i dipendenti sono previsti una serie di

incontri per garantire un'appropriata formazione riguardo alla conoscenza dei relativi obblighi previsti dalla normativa a carico di ciascun soggetto a cui la Legge stessa fa riferimento. Il corso verterà sui contenuti sostanziali della sicurezza con particolare accento alle responsabilità per il corretto trattamento dei dati.

Destinatari

Responsabili, a vari livelli, della gestione delle informazioni soggette alla privacy:

- Responsabili del trattamento
- Personale incaricato del trattamento dei dati

Contenuti del piano

Programma Analitico Corso Avanzato – I Giornata

Parte Generale

- Perché una formazione sulla Privacy?
- Il contesto storico –normativo della privacy
  - Il concetto di privacy
  - Che cosa significa privacy?
  - Il concetto di privacy nella storia e nella cultura
  - La storia della privacy nella cultura anglosassone
  - La storia della privacy in Italia
- Dal concetto alla normativa
  - La regolamentazione della privacy
  - La protezione della sfera privata della persona nella normativa
  - Il diritto della persona alla riservatezza della persona nella vita privata ed al controllo delle informazioni che la riguardano
- L'evoluzione della normativa
  - La prima regolamentazione: La legge 675/96 "Tutela della persona e di altri soggetti rispetto al trattamento dei dati personali"
  - Il d.lg. 318/99
  - Dalla 675/96 al Testo Unico sulla Privacy
- Il d.lg. 196/03 – Codice in materia di protezione dei dati personali
  - Le novità: modifiche ed integrazioni introdotte al precedente impianto normativo
    - L'impatto del Codice sul patrimonio informativo: novità e temi di rilievo
    - Impatto del Codice sul sistema di sicurezza: novità e temi di rilievo
  - La struttura del nuovo - Codice I Parte:
    - Principi Generali: Finalità, Necessità, Definizioni e Ambito di applicazione
    - Diritti dell'interessato
    - Regole Generali per il Trattamento dei Dati
    - I Soggetti del Trattamento
    - Gli adempimenti – La notificazione
    - Gli adempimenti – Le Misure di Sicurezza

- La struttura del nuovo Codice - II Parte
  - Disposizioni Relative a Specifici Settori
- La struttura del nuovo Codice - III Parte:
  - Tutela dell'Interessato e Sanzioni

Programma Analitico Corso Avanzato – II Giornata

La Sicurezza dei Dati: dal Dpr 318/99 all'"Allegato B"

- La sicurezza dei dati e dei sistemi
  - Le misure di sicurezza
    - Misure minime
    - Misure idonee
  - Le sanzioni
  - Sicurezza e integrità dei dati
  - Gli appalti e l'outsourcing
- Le nuove prescrizioni in materia di sicurezza
  - Misure logiche
  - Misure fisiche
  - Misure organizzative

Il DPsS e gli adempimenti connessi

- Il disciplinare tecnico in materia di trattamento dei dati personali
  - I filtri sull'accesso logico
    - Il sistema di autenticazione: identificazione dell'incaricato
    - Il sistema di autorizzazione: privilegi di accesso dell'incaricato
  - Le misure minime informatiche per i dati sanitari
  - I trattamenti cartacei
    - Regolamentazione degli accessi agli archivi
  - I mansionari per gli incaricati, le procedure, gli accorgimenti
- Gestire il problema della sicurezza dei dati negli Enti Locali
  - Il documento programmatico sulla sicurezza
    - Dalla distribuzione dei compiti all'elenco dei trattamenti
    - Le istruzioni per il responsabile
    - Le istruzioni per l'incaricato
    - Attività di vigilanza del titolare
  - L' analisi dei rischi
  - L'individuazione delle contromisure
  - Il piano di formazione del personale
  - Il salvataggio dei dati
  - Dispositivi antivirus, anti-intrusione e l'aggiornamento automatico degli applicativi
  - La dichiarazione di conformità

- Il piano di emergenza
  - La definizione del piano
  - L'individuazione degli applicativi coinvolti
  - I tempi di ripristino
  - La simulazione
- I tempi di adeguamento e le scadenze previste

Periodicità incontri

Diversi incontri sono previsti a partire dal 16/01/2006

8. CRITERI PER GARANTIRE L'ADOZIONE DELLE MISURE DI SICUREZZA IN CASO DI TRATTAMENTI AFFIDATI ALL'ESTERNO

Nell'atto di nomina, la Provincia di Benevento informa il Responsabile esterno circa i compiti che gli sono affidati in relazione a quanto previsto dalla normativa in vigore, con particolare riferimento a quanto stabilito dal Disciplinare Tecnico del Testo Unico.

Il Responsabile esterno si impegna a condurre su base periodica, almeno annuale, verifiche in merito all'osservanza della legge e delle istruzioni nelle operazioni di trattamento dei dati personali forniti dall' Ente.

Il Titolare si riserva la facoltà di verificare l'efficacia delle misure predisposte per la tutela dei dati dal Responsabile esterno.

9. ADOZIONE DI CONTROLLI PERIODICI

Il Titolare si impegna ad effettuare, con cadenza almeno annuale, controlli periodici sul contenuto del presente documento e sulle misure di sicurezza adottate.
A norma del Codice in materia di protezione dei dati personali, le misure minime di sicurezza adottate dalla Provincia di Benevento verranno adeguate periodicamente sulla base "dell'evoluzione tecnica del settore e dell'esperienza maturata", così come richiesto dall'art 36, comma 1 del Codice.

Con osservanza
Il Presidente della Provincia di Benevento
Titolare del trattamento

PROVINCIA DI BENEVENTO	DOCUMENTAZIONE PRIVACY	
	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA - Istruzione Operativa 1 - **PROCEDURA ACCESSI AL SISTEMA INFORMATIVO E GESTIONE DELLE POSTAZIONI DI LAVORO**	Revisione **1.2** Data **20/12/2005** Pagina **0** di **23**
Documento redatto da: CM Consit S.p.A.	**Documento verificato da:**	**Documento approvato da:**

1. STORIA DELLE MODIFICHE

Posizione	Descrizione della modifica
Versione 1	
Dicembre 2005	- Prima stesura

2. INDICE

3. SCOPO

Regolamentare le autorizzazioni all'accesso al Sistema Informativo e la gestione dei PDL onde proteggere il patrimonio dei dati della Azienda Ospedaliera Universitaria del II° Ateneo di Napoli (di seguito brevemente "ENTE") nel rispetto della normativa sulla protezione dei dati personali (D.Lgs. 30/06/2003 n° 196 "Codice in materia di protezione dei dati personali" e relativo allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza").
La mancata adozione delle misure minime di sicurezza è sanzionata penalmente dalla legge italiana.

4. VALIDITÀ

Le indicazioni contenute nella presente procedura si applicano al Sistema Informativo (HW e SW), nonché a tutti i dispositivi di informatica individuale utilizzati nell'ENTE.

5. RIFERIMENTI

[RIF1]	D.Lgs. 30/06/2003 n° 196 "Codice in materia di protezione dei dati personali"
[RIF2]	allegato B al D.Lgs. 196/03 "Disciplinare Tecnico in materia di misure minime di sicurezza".
[RIF3]	Documento Programmatico sulla Sicurezza
[RIF4]	ProvBn-VerbaleConsegnaCed - Verbale di consegna locali ced e procedure informatiche per il presidio ed affidamento del servizio sotto riserva di legge nelle more della stipula del contratto – Contratto Fornitura di servizi di presidio del Centro di Calcolo e manutenzione correttiva ed evolutiva del Sistema Informativo del Settore Amministrativo

6. DEFINIZIONI

Dati trattati nell'ENTE:	I dati trattati nell'ENTE da proteggere vengono classificati in 3 tipi: a) Dati personali: qualunque informazione relativa a persona fisica, giuridica, ente ed associazione (es. nome, cognome, indirizzo, ragione sociale, ecc.). b) Dati personali sensibili: dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, le adesioni a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute o la vita sessuale degli interessati c) Dati personali giudiziari d) Altri dati trattati nell'ENTE
Sistema Informativo:	Il Sistema Informativo si compone di: a) Applicazioni centralizzate. • Applicazioni gestite direttamente dal Servizio CED dell'ENTE. Queste possono essere sia applicativi del tipo "pacchetto" acquisito da un fornitore, che applicativi sviluppati all'interno dell'ENTE. I dati sono parte integrante dell'applicativo informatico. b) Archivi Utenti Condivisi. Archivi contenenti dati trattati dall'ENTE gestiti direttamente dai Reparti interessati e che si appoggiano sul Sistema Informativo dell'ENTE. I dati si trovano su supporti del tipo cartella LAN / disco condiviso e possono essere consultati e/o aggiornati da più persone. c) Informatica Individuale. Archivi gestiti sulla informatica individuale, tipicamente un PC o archivi personali in rete. Gli utenti devono seguire la procedura ISTR_BN01-01. I dati si trovano nella memoria del PC (supporto magnetico e altro).
Postazione Di Lavoro (PDL):	si intende qualunque dispositivo elettronico dotato di memoria capace di elaborare automaticamente dati (desktop, notebook, laptop, palmare, etc.)
Assegnatario di PDL:	ciascuna persona fisica (dipendente o esterna all'ENTE) alla quale viene assegnato una PDL in dotazione individuale.
Utente:	ciascuna persona fisica (dipendente o esterna all'ENTE) autorizzata all'accesso al Sistema Informativo.
Utenza:	è detta anche UserID o anche codice identificativo dell'utente. E' un codice individuale non riassegnabile per accedere ad uno specifico componente del Sistema Informativo. A ciascun utente si possono assegnare più utenze.

Profilo:	elenco delle procedure o servizi informatici alle quali ciascuna utenza è abilitata. E' specifico per ciascuna utenza. Può variare nel tempo, con le necessarie autorizzazioni, a seguito del modificarsi delle esigenze di lavoro dell'utente e della evoluzione del numero e del tipo delle procedure o servizi disponibili sul Sistema Informativo.
Procedure o servizi:	operazioni elementari informatiche consentite da parte del Sistema Informativo sui dati ivi registrati. Possono aversi procedure o servizi di sola consultazione e di consultazione ed aggiornamento.
Password di utenza:	È detta anche parola chiave di utenza. È un codice segreto individuale, scelto dall'utente per ogni utenza a lui assegnata e conosciuto solo dall'utente stesso. È necessario introdurla all'atto dell'accesso alla PDL, unitamente al proprio codice di utenza (altrimenti detto UserID o codice identificativo dell'utente), per accedere al componente del Sistema Informativo al quale l'utenza si riferisce. In tal modo viene garantito che l'utilizzo dell'utenza (e delle procedure o servizi informatici autorizzate per tale utenza) sia consentito solo al reale assegnatario.
Titolare del trattamento:	Vedi [RIF3]
Responsabili del trattamento:	Vedi [RIF3]
Incaricati del trattamento:	Vedi [RIF3]
Responsabile di area:	Chiunque abbia responsabilità di coordinamento di altro personale – in molti casi coincide con il Responsabile del Trattamento
Servizio CED	Ufficio a cui efferisce il personale addetto alla gestione dell'Infrastruttura IT dell'ENTE.
Addetti Sistema Informatico	Persone incaricate per iscritto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. Normalmente sono persone del CED della PROVINCIA L'addetto ha le autorizzazioni strettamente necessarie alla gestione dell'infrastruttura informativa e non ha i seguenti diritti che sono esclusivi dell' Amministratore di Sistema: o gestire l'infrastruttura a livello Enterprise; o accedere alle aree definite riservate; o accedere alla gestione delle mailbox della posta elettronica interna dell'ente, tipicamente utilizzata a livello di intranet o accedere alla gestione delle mailbox della posta elettronica fornite dall'ISP; o effettuare il recovery dei certificati digitali utilizzati per la cifratura dei dati e/o delle mail.
Amministratore di Sistema	Gestisce l'infrastruttura a livello Enterprise accede alle aree definite riservate; accede alle mailboxes della posta elettronica; effettua il recovery dei certificati digitali utilizzati per la cifratura dei dati e/o delle e-mail.
Tecnico di esercizio	È colui che ha le autorizzazioni strettamente necessarie alla risoluzione delle problematiche inerenti il funzionamento delle postazioni client.

7. REGOLE

7.1. Regole generali

7.1.1. Conferimento dell'incarico del trattamento di dati personali

Se l'assegnatario di PDL individuale e/o di utenza del Sistema Informativo deve trattare dati personali (e/o sensibili/giudiziari), egli deve essere nominato per iscritto "Incaricato del trattamento" con lettera a firma del Responsabile del trattamento.

7.1.2. Utilizzo delle risorse informatiche

Le PDL assegnate individualmente ai dipendenti e il Sistema Informativo devono essere utilizzati esclusivamente per gli scopi dell'ENTE.

L'accesso alle PDL assegnate individualmente ai dipendenti e al Sistema Informativo da parte degli utenti autorizzati deve essere sempre fatto attraverso l'utenza loro assegnata.

7.1.3. Utilizzo della posta elettronica e del trasferimento di file

Ciascun utente può utilizzare la posta elettronica e il trasferimento elettronico di file, verso destinatari interni o esterni all'ENTE, solo se la comunicazione è prevista dalla mansione ricoperta dall'utente stesso.

7.1.4. Regole di formazione delle password

La password deve avere le seguenti caratteristiche:

- Lunghezza minima 8 caratteri
- Non deve essere riconducibile al nome utente, nome/cognome reali, nome della società, data di nascita personale o dei familiari
- Non deve contenere parole compiute presenti nel dizionario.
- Deve essere significativamente diversa dalle password già utilizzate.
- Deve essere modificata al primo accesso al sistema
- Deve essere modificata successivamente ogni 90 giorni e l'utente viene avvisato dell'approssimarsi della scadenza a partire da 10 giorni prima.
- Il sistema deve tenere traccia delle password utilizzate ed impedirne il riutilizzo
- Se l'utente sbaglia per cinque volte la digitazione della password, il sistema disattiva automaticamente l'utenza per 30 minuti. Superato tale periodo l'utenza viene riattivata dal sistema.

7.1.5. Comportamento utente

Nel caso in cui l'utente si allontani dalla postazione di lavoro, la medesima deve essere bloccata.

In caso di non utilizzo della postazione da parte dell'utente superiore a 5 minuti, la postazione stessa si pone automaticamente nello stato di Lock. Per riattivare la sessione di lavoro l'utente deve effettuare di nuovo la procedura di login , digitando Username e Password.

7.1.6. Profili utente

Gli utenti sono identificati con il seguente criterio account:

- *Display Name*: Nome Cognome
- *Nome Account*: Nome.Cognome.NumeroMatricola (es. luigi.macalli.54601)

I sistemi operativi client supportano i profili utente. Per ogni utente vale quanto di seguito indicato:

- Un utente non ha diritti da amministratore sulla postazione di lavoro.
- Tutti gli "utenti locali" di ogni postazione sono disattivati.

- Il logon interattivo sulle postazioni di lavoro avviene utilizzando le credenziali dell'utente definito sul dominio.

Per ogni profilo utente sono definite:

- Unità di rete
- Stampanti di rete e locali
- Configurazione della posta elettronica
- Configurazione dei parametri del browser
- Restrizioni sull'utilizzo del software
- Modalità di aggiornamento del sistema operativo (patch, hot-fix)

7.1.7. Amministrazione Infrastruttura

- ✓ Gli account di amministrazione dell'infrastruttura, opportunamente rinominati con apposita codifica, sono conservati, con le relative password, in busta chiusa posta in cassaforte in un apposito faldone identificato con la scritta "privacy"

- ✓ Gli utenti incaricati di gestire l'infrastruttura accedono con il proprio account al quale vengono forniti i relativi diritti di amministrazione. Se è necessario operare sostanziali modifiche all'infrastruttura, sempre su delega e autorizzazione dell'amministratore di sistema, si potrà accedere alla busta di cui al precedente punto. A seguito di utilizzo degli account, di cui al precedente punto, le password dovranno essere modificate dall'amministratore di sistema.

7.1.8. Accesso in una situazione di emergenza alla PDL o all'utenza di un assegnatario assente.

Qualora un assegnatario sia impossibilitato a venire in un ufficio e ENTE abbia l'esigenza di accedere alla PDL o all'utenza individuale, il Responsabile di Area richiede per iscritto al Servizio CED di "forzare" l'utenza impostando una nuova password che dovrà essere comunicata alla persona incaricata di effettuare l'accesso, che potrà iniziare ad operare solo previa sostituzione della password con una diversa solo a lui nota.

Al ritorno dell'assegnatario, il Servizio CED provvede ad effettuare una nuova "forzatura" impostando una nuova password "di comodo" per l'assegnatario imponendogli il cambio password al primo accesso.

7.1.9. Applicazione degli aggiornamenti periodici di sicurezza.

Con frequenza live i software dei server, delle altre apparecchiature informatiche e delle PDL individuali devono essere aggiornati applicando le "patch" rese disponibili dal produttore volte a prevenire le vulnerabilità e a correggerne difetti.

7.1.10. Backup

Tutti i dati devono essere oggetto di salvataggio giornaliero con conservazione degli ultimi cinque salvataggi secondo la seguente schedulazione:

Lun: Backup completo

Mar, Mer, Gio, Ven, Sab: *Backup differenziale*

Dom: Backup ASR (di sistema e della directory)

Inoltre deve essere conservato il backup dell'ultimo giorno lavorativo di ogni mese per un periodo minimo di due anni.

I supporti informatici contenenti tali backup devono essere conservati in luogo sicuro diverso da quello del sistema informatico.

Il backup viene effettuato a cura del Servizio CED esclusivamente sui dati registrati nei server.

E' compito dell'utente effettuare backup giornalieri di eventuali dati presenti in copia unica nel disco fisso del PDL individuale. Tale backup individuale può essere evitato copiando al termine della giornata lavorativa i dati da salvare dal PDL individuale alla propria cartella riservata sul server.

7.1.11. Restore

In caso di indisponibilità dei dati per effetto di danneggiamento o perdita, il restore deve essere completato al massimo entro sette giorni dal momento dell'inizio dell'indisponibilità. E' fatto obbligo a chiunque accerti l'indisponibilità dei dati di informare con immediatezza il Servizio CED e comunque non oltre le ventiquattro ore.

7.2. Postazioni Di Lavoro

7.2.1. Installazione di software sulle PDL

La dotazione di software installato sulle PDL dal Servizio CED non può essere alterata dall'utente. Ogni installazione di nuovo software deve essere di norma effettuata dal Servizio CED dell'ENTE.

7.2.2. Account locali delle PDL

Gli account utente definiti localmente alle PDL devono essere disabilitati a cura del Servizio CED all'atto dell'assegnazione all'utente. Un'apposita politica di dominio imporrà la rinomina dell'account "Administrator" locale che dovrà essere dotato di password, formata secondo quanto specificato nella regola 7.1.4, che sarà la stessa per tutte le PDL e dovrà essere posta in busta chiusa e custodita a cura dell'Amministratore di sistema. Quest'ultimo potrà essere utilizzato solo ed esclusivamente in caso di emergenza, visto che, sempre attraverso la politica di dominio di cui sopra, gli addetti del CED potranno/dovranno utilizzare il proprio account per operare sulle PDL con il quale potranno accedere con diritti amministrativi.

7.2.3. Assegnazione di PDL individuale

Quando viene assegnato una PDL individuale (nuovo o proveniente da un precedente assegnatario) ad un assegnatario, il Servizio CED cancella mediante formattazione tutti i dati precedentemente registrati nella memoria fissa dell'elaboratore.

Non è consentito trasferire una PDL da un assegnatario ad un altro senza informare il Servizio CED. In tale circostanza il disco fisso va riformattato o comunque i dati in esso contenuti devono essere cancellati in modo da renderli tecnicamente non recuperabili.

7.2.4. Dismissione di PDL

Quando un assegnatario dismette una PDL a lui assegnata (per dimissioni, pensionamento, cambio di incarico ecc.), il Servizio CED provvede alla clonazione (ghost) dei file presenti nel disco fisso conservandolo in luogo sicuro.

L'eventuale accesso ai dati salvati viene autorizzato dal Responsabile del Area dell'assegnatario cedente del PDL.

7.2.5. Antivirus

Tutte le PDL individuali sono dotate di un programma antivirus fornito da una primaria ditta specializzata in tali prodotti.

Il Servizio CED provvede a scaricare giornalmente, in un repository centrale presente su di un server aziendale, gli aggiornamenti del programma e delle definizioni dei virus resi disponibili dal produttore

Al primo collegamento delle PDL, l'attivazione dell'aggiornamento viene effettuata automaticamente dal sistema.

L'assegnatario ha l'obbligo di non disattivare l'antivirus nel corso dell'utilizzo delle PDL.

7.2.6. Supporti informatici

I supporti informatici (floppy disk, nastri, dischi zip, dischi fissi delle PDL, dischi ottici, etc.) contenenti o che hanno contenuto dati personali sensibili possono essere riutilizzati (per registrare altri dati, per inviare dati a corrispondenti interni o esterni, per prestare il supporto informatico ad altri, etc.) solo previa cancellazione permanente (es.: formattazione completa) del supporto stesso. La formattazione veloce o la semplice cancellazione dei file non è autorizzata.

7.3. Applicazioni centralizzate

7.3.1. Regole generali

Nello sviluppo o modifica di applicativi, nonché nell'acquisizione di "pacchetti" da utilizzare nell'ENTE, particolare attenzione deve essere data al controllo di accesso per garantire il rispetto delle regole di questa procedura. Nei casi in cui ENTE debba acquisire "pacchetti" che non dispongono delle funzionalità necessarie per applicare queste regole, il Servizio CED deve specificare procedure alternative per garantire la protezione dei dati. Pertanto qualsiasi nuovo tipo di software deve essere validato e certificato dal Servizio CED dell'ENTE.

In taluni casi è necessario farsi rilasciare dal fornitore/installatore l'attestazione di conformità del prodotto/servizio alle disposizioni del disciplinare tecnico così come previsto al punto 25 dell'allegato B al dlgs 196/2003.

Ogni utenza del Sistema Informativo deve essere individuale ed assegnata ad una ben identificata persona fisica

Non sono consentite utenze di gruppo

Non è consentito riutilizzare il medesimo codice di utenza, riassegnandolo ad altra persona alla cessazione dell'utilizzo da parte del precedente assegnatario

Non è consentito utilizzare l'utenza di accesso da parte di persona diversa dall'assegnatario.

Qualora un'utenza non venga utilizzata per un periodo consecutivo di sei mesi, essa viene disattivata a cura del Servizio CED.

7.3.2. Assegnazione di una nuova utenza

L'apertura di una nuova utenza per un dipendente (all'atto dell'assunzione ovvero in un tempo successivo, al variare della mansione nell'ENTE) avviene a cura del Servizio CED, su proposta del Responsabile del Settore e dietro validazione del Settore Risorse Umane.

La apertura di una nuova utenza per una persona esterna all'ENTE (consulente, dipendente di un fornitore, etc.) avviene a cura del Servizio CED, su proposta del Responsabile del Settore che rappresenta il punto di riferimento nell'ENTE della persona esterna e dietro validazione dell'Ufficio Amministrazione del Personale.

Ad ogni nuova utenza va assegnato un profilo (ovviamente solo dove è applicabile) che limita le procedure o servizi a quelle per cui l'utente è stato autorizzato.

Qualora la nuova utenza preveda il trattamento di dati personali, occorre nominare "incaricato del trattamento" il nuovo utente, se già non è stato fatto (vedi paragrafo 7.1.1).

L'Ufficio del personale conserva per il personale dipendente e per il personale esterno la documentazione cartacea, rappresentata dalla lettera di conferimento di incarico di trattamento e dal modulo "Autorizzazione al trattamento di dati personali (vedi [ALL1] Modulo P1). L'originale della richiesta scritta di profilo di accesso è conservata dal Servizio CED.

7.3.3. Variazione di un'utenza esistente

Qualora le esigenze di accesso al Sistema Informativo dovessero variare (per effetto del variare delle mansioni nell'ENTE, della disponibilità di nuove procedure o servizi attivati dal Servizio CED, del variare dei compiti assegnati al personale esterno, etc.), il profilo dell'utente viene variato a cura del Servizio CED, su proposta del Responsabile di Area.

Non è necessario inviare al dipendente o al personale esterno una nuova lettera di conferimento di incarico, in quanto quella inviata a suo tempo già prevede l'ipotesi di variazioni del profilo di accesso.

L'Ufficio Amministrazione del personale conserva la documentazione cartacea della variazione, rappresentata dalla lettera di conferimento di incarico di trattamento e dal modulo "Autorizzazione al trattamento di dati personali" (vedi [ALL1] Modulo P1)

7.3.4. Cessazione di un'utenza

Al cessare delle condizioni per l'accesso al Sistema Informativo (cessazione dell'ENTE per il personale dipendente, termine del rapporto contrattuale per il personale esterno, variazione della mansione nell'ENTE per il personale dipendente, etc.), l'utenza deve essere prontamente disattivata a cura del Servizio CED, a seguito di una comunicazione tempestiva inviata dall'Ufficio Amministrazione del personale.

È responsabilità della Direzione competente comunicare al Servizio CED il verificarsi delle condizioni relative al cambio di mansione e il termine del contratto per il personale.

7.4. Archivi utenti condivisi

Nel caso di Archivi Utenti Condivisi (Share), oltre alle regole generali di cui al capitolo 7.1, vanno applicate le seguente regole, qualora nell'Archivio Utenti Condivisi siano registrati dati personali.

Se invece tali archivi non contengano dati personali, è sufficiente l'invio al Servizio CED di una richiesta tramite template elettronico che richieda l'apertura di un nuovo Archivio Utenti Condivisi e che assicuri che in esso non verranno registrati dati personali.

7.4.1. Responsabile dell'Archivio Utenti Condivisi.

Per ciascun Archivio Utenti Condivisi deve essere identificato un Responsabile del trattamento. Quest'ultimo potrà richiedere l'attivazione di un Archivio Utenti Condivisi, contenente solo dati del cui trattamento egli ha la responsabilità.

7.4.2. Richiesta al Servizio CED

La richiesta di creare un archivio condiviso deve essere formulata per iscritto dal Responsabile del trattamento ed inviata al Servizio CED.

La richiesta deve specificare:

- ✓ la tipologia dei dati;
- ✓ l'indicazione se trattasi di dati personali e/o di dati personali sensibili;
- ✓ l'elenco dei dipendenti che hanno diritto all'accesso;
- ✓ la durata dell'archivio.

7.4.3. Creazione dell'Archivio Utenti Condivisi

Nei casi in cui l'archivio si appoggia sul Sistema Informativo dell'ENTE, l'area condivisa va legata esclusivamente ai dipendenti elencati nella richiesta.

Eventuali variazioni dei dipendenti con diritto di accesso vanno comunicate come indicato sopra

7.4.4. Alla scadenza della durata

Alla scadenza della durata, e nel caso in cui non venga richiesto per iscritto dal Responsabile del trattamento un prolungamento, il Servizio CED provvede alla storicizzazione e cancellazione dell'Archivio Utenti Condivisi, previo un preavviso al Responsabile del trattamento.

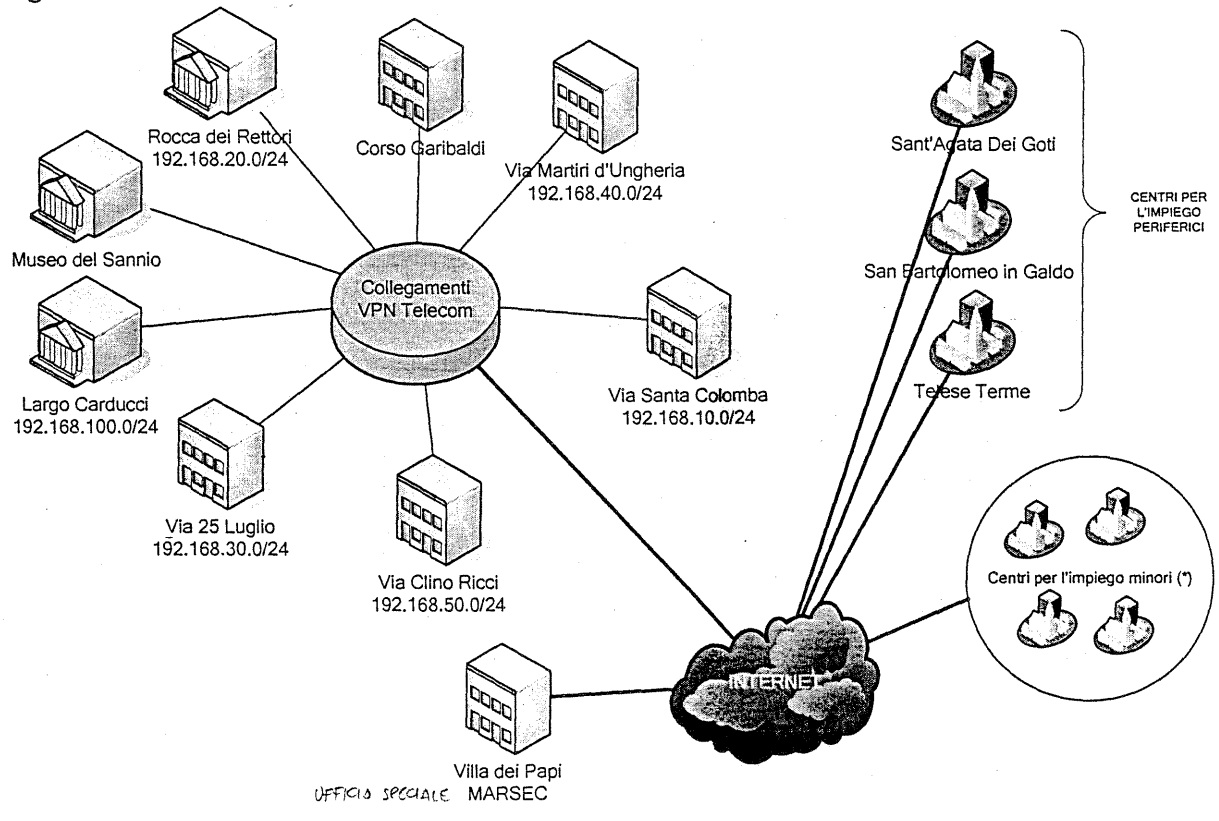
8. CONTESTO DI APPLICAZIONE: INFRASTRUTTURA DELLA DIRECTORY E CONFIGURAZIONE RETE LAN

Il sistema di lavoro della struttura avviene con elaborazione in rete privata/pubblica la cui specifica è di seguito descritta:

8.1. L'Infrastruttura di Rete

Si dispone di una rete, realizzata mediante collegamenti via cavo come di seguito schematizzata:

Fig.1



(*) I Centri per l'Impiego minori sono gestiti da personale dei centri per l'impiego periferici e non tutti dispongono di connettività verso internet.

Nell'ambito dell'infrastruttura di rete alcuni siti non sono serviti da un collegamento di "Campus" con connessioni gestite da Telecom e basate su collegamenti in modalità VPN (Virtual Private Network). Per tale motivo, per tali siti non è ipotizzabile un applicazione di politiche di sicurezza centralizzate, anche se ciò sarebbe possibile attraverso l'implementazione di canali di comunicazione protetta su internet (da tali siti verso la sede principale) realizzati con gli apparati di connettività esistenti e con opportune configurazioni

effettuate sui server del CED (VPN in modalità PPTP o L2TP/IPsec) e che vedranno la loro realizzazione entro Marzo 2006.
Attualmente la banda per le comunicazioni fra le sedi servite da tali collegamenti, è ***da ritenersi insufficiente*** visto che viene utilizzata sia per le comunicazioni da e verso il CED che per la connettività Internet. Fra l'altro nell'ottica di implementazione di siti per il ***disaster recovery,*** che potrebbero essere individuati nelle seguenti sedi:

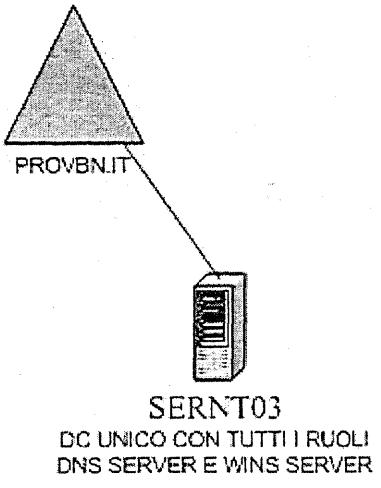
- Viale Martiri di Ungheria sede della Polizia Provinciale
- Via 25 Luglio sede del Centro per l'impiego di Benevento

sarebbe auspicabile un collegamento con una banda di almeno 2 mbps (anche se la situazione ottimale dovrebbe prevedere una connettività a partire da 6 mbps) per garantire la replica dei dati in tempo reale o almeno con uno scarto non superiore a 10 min.

8.2. L'Infrastruttura dei Domini di Sicurezza

Il servizio Directory è implementato utilizzando Active Directory di Microsoft Windows Server 2003. La Struttura dei ***domini di sicurezza*** attuale è di seguito rappresentata:

Fig.2



e può essere descritta sinteticamente come segue:

- ✓ L'infrastruttura conta un dominio di sicurezza.
- ✓ Il dominio permette l'accesso al proprio ambito di sicurezza solamente ed unicamente tramite l'identificazione univoca di un utente (con combinazione username/password – user account) e di una PDL (computer account).
- ✓ Sia gli utenti che le PDL sono aggiunti al dominio dall'amministratore di sistema o da un altro Amministratore IT delegato. Senza combinazione Username/Password valide in un ambito non e' possibile accedere, come non e' possibile accedere utilizzando PDL non aggiunte all'ambito di sicurezza da un amministratore.
- ✓ Gli utenti sono organizzati per gruppi di sicurezza (Domain Local) locali ai domini
- ✓ I permessi di accesso ai dati presenti sui server sono stabiliti a livello di File System e concessi ai gruppi di sicurezza in relazione al livello di accesso che gli utenti devono avere sui dati stessi
- ✓ Gli utenti e le PDL sono organizzate secondo uno schema di Unità Organizzative UO, mappata sul modello organizzativo dell'Azienda (in termini di plessi, settori e servizi) sulle quali vengono imposte apposite politiche di gruppo (GPO) che possono

essere generali per tutti gli utenti o particolareggiate allo scopo di restringere le autorizzazioni al trattamento dei dati a particolari classi e/o gruppi di utenti. Attraverso le GPO s'intende rendere gestibile centralmente l'intera struttura dell'ENTE imponendo un utilizzo in sicurezza delle PDL connesse all'infrastruttura.

- ✓ Il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione attraverso:
  - o l'implementazione di un server WSUS attraverso il quale vengono scaricate le Hot Fix e gli aggiornamenti dal sito Microsoft ed effettuato il deployment su tutti i client dell'infrastruttura. Quest'ultimo è imposto sulle workstation di dominio a livello di policy. L'amministratore di sistema ha il compito di approvare per il deploy gli aggiornamenti scaricati sul server WSUS. La pubblicazione di un nuovo aggiornamento viene notificata da Microsoft all'amministratore di sistema attraverso una e-mail identificata come "Security Update"
  - o L'installazione, lato server, di un repository per gli update dell'antivirus. Tale repository viene referenziato dal software antivirus installato sui client così configurato per gli aggiornamenti delle definizioni dei nuovi virus/worm.
  - o Agli incaricati è stato affidato il compito di verificare, con cadenza settimanale che il sistema di protezione sia correttamente aggiornato.

L'infrastruttura attuale, anche se formalmente rispetta i requisiti minimi per l'adozione delle misure minime di sicurezza previste dall'allegato B al Dlgs 196/2003, presenta diversi SPOF (Single Point Of Failure), uno fra tutti la presenza di un unico server con funzioni di Controllore di Dominio e unico proprietario di tutti i ruoli compresi quelli per la gestione del naming delle PDL (DNS e Wins).

Per tal motivo, a breve, e comunque non oltre il 31/06/2006 l'intera infrastruttura subirà una radicale reingegnerizzazione in termini di

- disegno
- sicurezza
- disaster recovery policy
- Group Policy Modelling.

9. IL SISTEMA INFORMATIVO AZIENDALE

Il sistema informativo aziendale è composto dalle seguenti applicazioni centralizzate, gestite dal servizio CED:

Sottosistema di Contabilità Economico-Finanziaria

Applicazione/ modulo software	Descrizione	Piattaforma operativa	Base Dati
SIEP COFI	Applicazione integrata per la gestione della contabilità finanziaria secondo il DL. 77 ed economico-patrimoniale	SCO UNIX - MicroFocus Cobol	C-Isam
SIEP OnLine	Applicazione per l'analisi finanziaria dei capitoli di bilancio per ciascun settore	Windows – VB Microsoft	SQL Server
TxTitoli	Modulo software integrato in SIEP per la trasmissione digitale dei titoli alla banca tesoriera	SCO UNIX - MicroFocus Cobol	C-Isam
SIOPE	Modulo software integrato in SIEP per l'adeguamento dei files relativi alla trasmissione dei titoli alla banca secondo le specifiche del Ministero dell'economia e delle finanze. E' in fase di implementazione.	SCO UNIX - MicroFocus Cobol	C-Isam
Quietanze	Modulo software integrato in SIEP per l'acquisizione delle quietanze di pagamento direttamente dalla banca tesoriera. L'applicazione dovrà essere implementata in funzione delle nuove specifiche richieste dalla banca tesoriera.	SCO UNIX - MicroFocus Cobol	C-Isam
Bilancio Previsionale	Modulo software per la gestione del PEG. Il modulo permette le imputazioni previsionali per ciascun settore su appositi fogli di calcolo excel. Successivamente detti dati vengono elaborati e caricati, tramite apposita interfaccia, nel DataBase dell'applicazione SIEP per la formazione del Bilancio Previsionale.	Windows – VB Excel SCO UNIX - MicroFocus Cobol	SQL Server C-Isam

Bilancio XML	Modulo software per la gestione dei bilanci da trasmettere alla Corte dei Conti in formato XML secondo le specifiche della normativa vigente. Il software è stato realizzato internamente al servizio CED. L'implementazione del modulo software risulta ancora nella fase di verifica funzionale e andrà ad essere completata in funzione dei test operativi in corso.	SCO UNIX - MicroFocus Cobol Windows – VB Microsoft Altova XML Spy	C-Isam SQL server

Sottosistema delle Risorse Umane

Applicazione/ modulo software	Descrizione	Piattaforma operativa	Base Dati
SIEP HR	Applicazione integrata per la gestione delle paghe e stipendi per il personale della Provincia	SCO UNIX - MicroFocus Cobol	C-Isam
Scioglimenti e Determine	Applicazione per la gestione dei costi del personale con analisi per centro di costo ed elaborazione delle determine sui capitoli di competenza per entrate e uscite sui conti del personale. L'applicazione si integra con la banca dati del SIEP per ricevere le voci mensili di costo e ritenute.	Windows – VB Microsoft SCO UNIX - MicroFocus Cobol	SQL Server C-Isam
Cedolino On-Line	Applicazione che permette l'imputazione delle voci mobili di cedolino da computare mensilmente sulle paghe. Tali voci sono inserite, tramite apposita interfaccia, direttamente nell'applicazione SIEP HR.	Windows – VB Microsoft SCO UNIX - MicroFocus Cobol	SQL Server C-Isam
INAZ RIO	Applicazione per la gestione delle presenze assenze del personale della Provincia. Il software è realizzato dalla società INAZ paghe.	Windows – VB Microsoft	SQL Server
SIGMA	Applicazione integrata per la gestione giuridica del personale. Il software è integrato nelle applicazioni SIEP HR e INAZ RIO.	Windows – VB Microsoft	SQL Server
TRASFERTE	Applicazione Web per la gestione delle trasferte dei dipendenti. Permette l'imputazione delle voci di	Windows Dot.Net	SQLServer

	trasferta con il calcolo automatico delle indennità e dei costi spettanti, secondo uno specifico procedimento autorizzativo. L'applicazione è in fase di messa in esercizio.		
Giornaliera	Applicazione per la giustificazione delle timbrature mancanti. E' utilizzata dalle segreterie di direzione.	Windows – VB Microsoft	SQL Server

Sottosistema del Settore Agricoltura

Applicazione/ modulo software	Descrizione	Piattaforma operativa	Base Dati
POR Gest	Applicazione integrata per la gestione dei progetti POR agricoltura . L'applicazione è manutenuta dalla Regione Campania. Il servizio CED ne garantisce l'esercizio e le installazioni ed aggiornamenti che periodicamente invia la Regione.	Windows – VB Microsoft	Oracle
WebSMI	Applicazione web per la gestione informatizzata dei flussi finanziari dalle dichiarazioni del beneficiario finale fino ai soggetti responsabili dell'attuazione delle misure coofinanziate. Il software applicativo è realizzato dalla Regione Campania tramite la società Studio Staff. Ad oggi risulta una prima installazione effettuata dalla Regione con la società Studio Staff sui sistemi della Provincia.	Microsoft ASP.NET	Microsoft SQL Server 2000
UMA	Applicazione per la gestione dei motori e macchine agricole.	Windows – VB Microsoft	SQL Server

Altri sottosistemi distribuiti per la gestione applicativa

Applicazione/ modulo software	Descrizione	Piattaforma operativa	Base Dati
Protocollo Elettronico	Applicazione integrata per la gestione del protocollo elettronico secondo il DPR. 445/2000. L'applicazione è usata limitatamente alle funzionalità previste per il "Nucleo Minimo" (norme CNIPA e DPR 445/2000). Prevede la possibilità di configurare un sistema di Work Flow management secondo le linee guida emanate dal CNIPA. Le funzionalità descritte, seppure disponibili sull'attuale piattaforma, non risultano ad oggi configurate e personalizzate per l'utilizzo presso la Provincia di Benevento.	Windows – Lotus Domino Server	LotusDomino
Mail Interna	Applicazione per la gestione della posta elettronica interna per tutte le postazioni di lavoro collegate alla rete Intranet della Provincia	Windows – Lotus Domino Server	LotusDomino

Altri sottosistemi distribuiti per la gestione della rete dati e i collegamenti con le sedi periferiche della Provincia

Applicazione/ modulo software	Descrizione	Piattaforma operativa	Base Dati
Antivirus: Norton Corporate	Applicazione centralizzata per la distribuzione automatica e aggiornamento delle impronte virali per la protezione da virus	Windows server	
Proxy server	Applicazioni Proxy per il controllo del traffico Internet per tutte le sedi collegate alla rete VPN della Provincia. I sistemi sono mantenuti dal CED.	Linux Debian	

Modalità di accesso alle applicazioni (*)

Applicazione	*Modalità di Accesso*		*Lunghezza Minima Password*	*Gestione Profili Utente*	*Gestione Scadenza Password*	*Gestione Password*
	UserID	*PSW*				
SIEP COFI	X	X	0	Si	No	CED
SIEP online	X	X	0	Si	No	CED
TxTitoli	X	X	0	Si	No	CED
SIOPE	X	X	0	Si	No	CED
Quietanze	X	X	0	Si	No	CED
Bilancio Previsionale	X	X	0	Si	No	CED
Bilancio XML	X	X	0	Si	No	CED
SIEP HR	X	X	0	Si	No	CED
Scioglimenti e Determine	X	X	0	Si	No	CED
Cedolino On-Line	X	X	0	Si	No	CED
INAZ RIO	X	X	0 max 10	No	No	CED
SIGMA	X	X	0	Si	No	CED
TRASFERTE	X	X	0	Si	No	CED
Giornaliera	X	X	0	Si	No	CED
POR Gest	X	X	0 max 10	No	No	CED
WebSMI	X	X	0 max 10	No	No	CED
UMA	X	X	0 max 10	No	No	CED
Protocollo Elettronico	X	X	0 Abilitabile 8 Char	Si	No Abilitabile	UTENTE
Mail Interna	X	X	0 Abilitabile 8 Char	No	No Abilitabile	UTENTE

(*) Per tutte le applicazione dove non è prevista una gestione della lunghezza minima delle password e della scadenza delle stesse dovranno essere oggetto di manutenzione evolutiva per renderle conformi al disciplinare tecnico previsto nell'allegato B al Dlgs 196/2003

10. COMPITI E RESPONSABILITÀ

10.1. Responsabile di Area ([1])

Ha il compito di illustrare ai propri collaboratori le responsabilità a questi assegnate nel trattamento di dati personali.

Questa attività di formazione deve essere svolta soprattutto quando il collaboratore venga autorizzato all'accesso a procedure o servizi operanti su dati sensibili, nonché per nuovi assunti e cambi di attività significativi.

Assicura che le PDL individuali siano assegnate a persone definite

Qualora una PDL assegnata all'Area debba essere trasferita da un assegnatario ad un altro, applica quanto previsto nel paragrafo 7.2 e, in quest'ambito, assicura che i dati contenuti nel disco fisso debbano essere comunicati al nuovo assegnatario, in quanto incaricato del medesimo trattamento. In caso negativo, assicura che i dati siano cancellati in modo permanente.

Valuta le esigenze di accesso del proprio dipendente alle procedure o servizi disponibili sul Sistema Informativo e sottopone all'approvazione del Responsabile del trattamento il modulo di autorizzazione all'accesso ([ALL1] - Mod. P1), sia per l'attivazione di nuova utenza, che per variazione delle procedure o servizi autorizzate per utenze preesistenti.

Valuta le esigenze di accesso alle procedure o servizi disponibili sul Sistema Informativo del personale esterno a ENTE (lavoratori temporanei, consulenti, dipendenti di fornitori, etc.), del quale rappresenta il punto di riferimento nell'ENTE, e sottopone all'approvazione del Responsabile del trattamento il modulo di autorizzazione all'accesso ([ALL1] - Mod. P1), sia per l'attivazione di nuova utenza, che per variazione delle procedure o servizi autorizzati (per accedere a nuove procedure o servizi e disattivare accessi precedentemente attivati).

Qualora si tratti di prima autorizzazione all'accesso a dati personali per il dipendente o per il personale esterno, predispone la lettera di conferimento dell'incarico del trattamento di dati personali (vedi [RIF3]) e la sottopone alla firma del Responsabile del Trattamento.

Nel caso di cui al comma precedente, consegna la lettera di conferimento di incarico al dipendente o al personale esterno e ne ottiene la firma per ricevuta.

Trasmette l'originale del modulo approvato (di cui al punto e) o f)) al Servizio CED per l'attivazione e/o la modifica e/o l'integrazione del profilo di accesso.

Invia una copia del modulo stesso all'Ufficio Amministrazione del personale, unitamente alla copia della lettera di conferimento di incarico con la firma per ricevuta (qualora si ricada nell'ipotesi di cui al comma g)), per l'archiviazione nella cartella personale. Comunica al Servizio CED il manifestarsi della condizione di revoca dell'utenza per il personale esterno di cui egli rappresenta il punto di riferimento nell'ENTE.

Comunica al Servizio CED le assenze prolungate (maternità, malattia, corsi all'estero, etc.) del personale dipendente, affinché siano disattivate temporaneamente tutte le utenze del dipendente.

10.2. Responsabile del trattamento

Approva l'attivazione e/o variazione delle utenze assegnate al personale dipendente facente parte della sua Direzione e delle utenze assegnate al personale esterno di competenza.

Sottoscrive la lettera di conferimento di incarico di trattamento.

Annualmente controlla e approva tutti gli accessi autorizzati alle banche dati di competenza, sulla base della documentazione disponibile sul Sistema Informativo.

[1] Vedi Cap.6 – Definizioni

10.3. Servizio CED dell'ENTE

All'atto dell'installazione di una nuova PDL ad un assegnatario:

- si accerta che sul disco fisso non siano presenti dati personali di precedenti assegnatari;
- attiva la protezione antivirus installando l'ultima versione disponibile del software antivirus prescelto;
- si accerta che siano installate tutte le "patch" di sicurezza rilasciate dal produttore per i software installati;
- attiva la protezione delle PDL d'ufficio mediante password dell'utente locale "administrator" che rispetti le regole di cui al punto 7.2.2;
- nel caso di PDL portatili crea un utente locale protetto da password e la comunica all'utente che provvederà immediatamente a modificarla con altra segreta che rispetti le medesime regole di cui al punto 7.1.4;
- attiva una protezione sulla cartella "Documenti" onde consentire l'accesso esclusivo dell'assegnatario a tale cartella, nel caso di computer portatili a tale cartella dovrà poter accedere sia l'utente di rete che l'utente locale della PDL in modo tale da permettere all'assegnatario di lavorare sugli stessi file locali indifferentemente da uno o l'altro utente.

Rende disponibile con tempestività a tutti gli assegnatari di PDL gli aggiornamenti del software antivirus e delle definizioni dei virus resi disponibili dal produttore.

Comunica ai Responsabili di Area potenzialmente interessati l'attivazione di nuove procedure o servizi e/o la cessazione di procedure o servizi prima disponibili.

Sulla base delle richieste di attivazione/modifica di utenza, provvede all'assegnazione del codice di utente (per le nuove utenze) ed all'attivazione/disattivazione delle procedure o servizi sulla base dell'autorizzazione.

Archivia una copia dei moduli di richiesta di attivazione/modifica di utenza relativi al dipendente e al personale esterno.

Mantiene una situazione aggiornata delle utenze attive, con indicazione dell'utente e delle procedure o servizi alle quali egli è autorizzato.

Mantiene una situazione storica di tutte le utenze assegnate e delle variazioni nel tempo intervenute per ciascuna (data attivazione/data cessazione dell'utenza).

Disattiva automaticamente tutte le utenze che non sono utilizzate per un periodo consecutivo di sei mesi.

Con frequenza almeno annuale richiede a ogni Responsabile del trattamento la verifica della validità di tutte le autorizzazioni di accesso attive per le banche dati di competenza.

10.4. Ufficio Amministrazione del Personale dell'ENTE

Archivia la copia della lettera di conferimento di incarico controfirmata per ricevuta dal dipendente.

Archivia la copia della lettera di conferimento di incarico al personale non dipendente controfirmata per ricevuta e accettazione.

Comunica al Servizio CED le cessazioni, affinché si provveda alla disattivazione di tutte le utenze assegnate al cessato.

10.5. Assegnatario di PDL

Nel caso che sia assegnatario di PDL d'ufficio accederà al medesimo solo attraverso la sua utenza di rete.

Nel caso che sia assegnatario di PDL portatile quando sarà presente presso ENTE accederà al medesimo solo attraverso la sua utenza di rete, in tutti gli altri casi potrà accedere con l'utente locale della PDL.

Nel caso che sia assegnatario di PDL portatile, installa, con cadenza almeno settimanale, gli aggiornamenti del software antivirus resi disponibili sul server dal Servizio CED.

Mantiene sempre attiva la protezione antivirus sul proprio PDL.

Spegne il PDL assegnato, ogniqualvolta si allontana dal posto di lavoro. In alternativa, è consentito, in occasione di assenze durante l'orario di lavoro, proteggere l'accesso al PDL mediante procedura di "Log-Off".

10.6. Utente

Riceve l'autorizzazione di accesso alle procedure o servizi del Sistema Informativo, con il relativo codice utenza (UserID) e password di utenza iniziale a lui assegnata.

Modifica la password iniziale di utenza, seguendone le regole per la formazione di cui al punto 7.1.4. Le password di utenza possono essere diverse per ciascuna utenza.

Accede alle procedure o servizi del Sistema Informativo, introducendo il proprio codice utenza (UserID) seguito dalla relativa password di utenza. Non è consentito accedere contemporaneamente alle procedure o servizi del Sistema Informativo da due postazioni diverse.

Conserva le password con la massima cura e non le comunica a nessuno all'interno ed all'esterno dell'ENTE.

Modifica almeno ogni 90 giorni la password di accesso alla rete ed almeno (la scadenza verrà imposta automaticamente dalle policy di dominio dell'infrastruttura).

In ogni caso modifica immediatamente la password ogniqualvolta che essa venga portata a conoscenza di terzi per qualsiasi motivo.

Disattiva l'accesso al Sistema Informativo ogniqualvolta si allontana dal posto di lavoro.

11. ALLEGATI

[ALL1] P1 Autorizzazione al trattamento di dati personali.

Allegato P1
(Esempio)

Autorizzazione al trattamento di dati personali

Utente	Cognome	Nome	Reparto interno o Azienda esterna

Categoria utente	Dipendente	Consulente	Dipendente di fornitore	

Banche dati cartacee

Applicazioni informatiche

Utenza:	❑	❑	❑

❑ **Nuova utenza**	❑ **Modifica di utenza**	❑ **Cessazione di utenza**

Funzioni	Codice	Denominazione	Lettura	Lettura/ Scrittura

Richieste ed autorizzazioni

Dipendente o consulente	Cognome e Nome	Firma	Data

Responsabile del trattamento competente	Cognome e Nome	Firma	Data

Servizio CED	Cognome Nome	Firma	Data