Studio Cardella

Ing. Angelo Cardella

DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI

Adozione delle Misure Minime di Sicurezza previste nell'Allegato B al D. Lgs. 196/03 "Disciplinare tecnico in materia di misure minime di sicurezza"

Ai sensi del Decreto Legislativo n. 196 del 30 Giugno 2003 - "Codice in materia di protezione dei dati personali" e successive modifiche e integrazioni

Ordine degli Ingegneri

Provincia di Caltanissetta

Viale Trieste, 281

93100 - Caltanissetta

Codice Fiscale: 80005220852

opec271.20161021120442.20875.03.1.03.18@pec.aruba.it

Caltanissetta, 21 Ottobre 2016

Riferimenti Normativi

Il presente documento nell'ambito dell'aggiornamento con cadenza almeno annuale della lista degli incaricati, degli addetti alla gestione e manutenzione degli strumenti elettronici dei trattamenti consentiti agli incaricati è redatto ai sensi del Decreto Legislativo n. 196 del 30 Giugno 2003 ed aggiornato in base ai seguenti provvedimenti:

- decreto legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla Legge 17 aprile 2015, n. 43;
- legge 27 dicembre 2013, n. 147;
- decreto legislativo 14 marzo 2013, n. 33
- decreto legislativo 28 maggio 2012, n. 69;
- decreto legge 9 febbraio 2012, n. 5,
convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35;
- decreto legge 6 dicembre 2011, n. 201,
convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214;
- decreto legge 13 maggio 2011, n. 70
convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106;
- legge 4 novembre 2010, n. 183;
- legge 29 luglio 2010, n. 120;
- decreto-legge del 25 settembre 2009, n. 135
convertito, con modificazioni, dalla legge 20 novembre 2009, n. 166;
- legge 4 marzo 2009, n. 15;
- decreto-legge del 30 dicembre 2008, n. 207
convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14;
- decreto-legge 25 giugno 2008, n. 112
convertito, con modificazioni, dalla legge 6 agosto 2008 n. 133;
- decreto legislativo 30 maggio 2008, n. 109;
- legge 18 marzo 2008, n. 48, ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
- decreto-legge 28 dicembre 2006, n. 300
convertito, con modificazioni, dalla legge 26 febbraio 2007, n. 17;
- decreto-legge 12 maggio 2006, n. 173
convertito, con modificazioni, dalla legge 12 luglio 2006, n. 228;
- decreto-legge 30 dicembre 2005, n. 273
convertito, con modificazioni, dalla legge 23 febbraio 2006, n. 51;
- decreto legge 30 novembre 2005, n. 245

convertito, con modificazioni, dalla legge 27 gennaio 2006, n. 21;

• decreto legislativo 7 settembre 2005, n. 209;

• decreto-legge 27 luglio 2005, n. 144

convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;

• decreto-legge 30 dicembre 2004, n. 314

convertito, con modificazioni, dalla legge 1 marzo 2005, n. 26;

• decreto-legge 9 novembre 2004, n. 66

convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 306;

• decreto-legge 24 giugno 2004, n. 158

convertito, con modificazioni, dalla legge 27 luglio 2004, n. 188;

• decreto-legge 29 marzo 2004, n. 81

convertito, con modificazioni, dalla legge 26 maggio 2004, n. 138;

• decreto legislativo 22 gennaio 2004, n. 42;

• decreto-legge 24 dicembre 2003, n. 354 convertito, con modificazioni, dalla legge 26 febbraio 2004, n. 45

DEFINIZIONI

Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Dato personale

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati sensibili

I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati giudiziari

I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Titolare

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Incaricati

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dato anonimo

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Blocco

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca dati

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Comunicazione elettronica

Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.
Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Misure minime

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione

I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica.

Parola chiave

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione

L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

NOMINA, RUOLI E COMPITI DELLE FIGURE PREVISTE PER LA SICUREZZA DEI DATI PERSONALI

Titolare del Trattamento dei Dati Personali:

Ordine degli Ingegneri della Provincia di Caltanissetta

P. IVA 80005220852

Viale Trieste, 281 - 93100 - Caltanissetta

Piazza San Francesco, 2 - 93012 - Gela

In base a quanto stabilito dall'**Art. 4, comma 1, lettera f) del Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 30 giugno 2003)** il "***Titolare del Trattamento*** *è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*".

Il **Titolare del Trattamento** si impegna ad assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del **Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.Lgs. n. 196 del 30 giugno 2003)** tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il **Titolare del Trattamento** può decidere, qualora lo ritenga opportuno, di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.

In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 30 giugno 2003)**, il **Titolare del Trattamento**, ove necessario, per esigenze organizzative, può designare facoltativamente uno o più soggetti **Responsabili del Trattamento** anche mediante suddivisione di compiti.

Finalità del Trattamento

"Il Trattamento:

- **È diretto al fine istituzionale della tenuta dell'Albo;**
- **È diretto all'adempimento di specifiche norme di legge (es. in materia contabile, fiscale, rapporto di lavoro etc.) o regolamenti (es. comunicazione Enti e Ministeri);**
- **È diretto al servizio di consulenza e assistenza agli iscritti all'ordine;**
- **È diretto al fine di promuovere attività di formazione e aggiornamento di tipo seminariale per gli iscritti. "**

Responsabili del Trattamento dei Dati Personali:

Bruno Giovanna Letizia

Il **Responsabile del Trattamento** è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

I compiti affidati al **Responsabile del Trattamento** sono analiticamente specificati per iscritto dal **Titolare del Trattamento**.

Il **Responsabile del Trattamento** effettua il trattamento attenendosi alle istruzioni impartite dal **Titolare del Trattamento**.

Qualora il **Titolare del Trattamento** ritenga di non nominare alcun **Responsabile del Trattamento**, ne assumerà tutte le responsabilità e funzioni.
In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 30 giugno 2003)**, il **Titolare del Trattamento**, ove necessario, per esigenze organizzative, può designare facoltativamente uno o più soggetti **Responsabili del Trattamento** anche mediante suddivisione di compiti.

Il Responsabile del Trattamento dei Dati Personali è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui da parte del **Titolare del Trattamento**, sono affidate le seguenti responsabilità e compiti:

- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco degli uffici in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
- Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.

- Redigere e di aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati.
- Nominare per ciascun ufficio in cui viene effettuato il trattamento dei dati, un **incaricato** con il compito di controllare i sistemi, le apparecchiature, e se previsti, i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
- Definire e verificare periodicamente le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.
- Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati della custodia delle copie delle credenziali** qualora vi sia più di un incaricato del trattamento.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati delle copie di sicurezza delle banche dati**.
- Custodire e conservare i supporti utilizzati per le copie dei dati.

Qualora il **Titolare del Trattamento** ritenga di non nominare alcun **Responsabile del Trattamento dei Dati Personali**, ne assumerà tutte le responsabilità e funzioni.

Amministratore di Sistema per la gestione e la manutenzione degli strumenti elettronici

Bruno Giovanna Letizia
Pecoraro Valeriano

In conformità a quanto disposto dal **punto 15, punto 16, punto 17 e punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)** il **Responsabile della sicurezza dei dati personali**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**.

L'**incaricato della gestione e della manutenzione degli strumenti elettronici** è la persona fisica che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di **Banche di dati**.

E' onere del **Responsabile della sicurezza dei dati personali**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**.

E' compito degli **Incaricati della gestione e della manutenzione degli strumenti elettronici**:

- Attivare per tutti i trattamenti effettuati con strumenti elettronici le **Credenziali di autenticazione** assegnate agli **Incaricati del Trattamento,** su indicazione del **Responsabile del Trattamento di dati personali**.
- In conformità a quanto disposto dal **punto 16 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)** definire l'attivazione di idonei strumenti per la protezione contro il rischio di intrusione e dell'azione di programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Questi strumenti debbono essere aggiornati con cadenza almeno semestrale.
- In conformità a quanto disposto dal **punto 17 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)**

aggiornare periodicamente (almeno una volta l'anno) i programmi per elaboratore per prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

- In conformità a quanto disposto dal **punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)** proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso da parte di chiunque abusivamente si introduce nel sistema informatico o telematico (art. 615-ter del Codice Penale).
- Informare il **Responsabile della sicurezza dei dati personali** nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato della gestione e della manutenzione degli strumenti elettronici**, ne assumerà tutte le responsabilità e funzioni.

Il **Responsabile della sicurezza dei dati personali** nomina uno o più soggetti **Incaricati della gestione e della manutenzione degli strumenti elettronici** a cui è conferito il compito di sovrintendere al buon funzionamento delle risorse del sistema informativo e degli accessi alle **Banche di dati**.

Anche se non espressamente previsto dalla norma, è opportuno che il **Responsabile della sicurezza dei dati personali** nomini uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

Il **Responsabile della sicurezza dei dati personali** deve informare ciascun **Incaricato della gestione e della manutenzione degli strumenti elettronici** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al D.Lgs. n. 196 del 30 giugno 2003)**.

La nomina di uno o più **Amministratori di Sistema** Incaricati della gestione e della manutenzione degli strumenti elettronici deve essere effettuata con una lettera di incarico e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Incaricato della gestione e della manutenzione degli strumenti elettronici** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina dell'**Incaricato della gestione e della manutenzione degli strumenti elettronici** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina degli **Incaricati della gestione e della manutenzione degli strumenti elettronici** può essere revocata in qualsiasi momento dal **Responsabile della sicurezza dei dati personali** senza preavviso, ed eventualmente affidata ad altro soggetto.

Incaricato della custodia delle copie delle credenziali

Bruno Giovanna Letizia

In conformità a quanto disposto dal **punto 10 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)** debbono essere impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il **Titolare del Trattamento** può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

E' onere del **Titolare del Trattamento** o, se designato, del **Responsabile della sicurezza dei dati personali**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della custodia delle copie delle credenziali**.

E' compito degli **Incaricati della custodia delle copie delle credenziali**:

- Autorizzare l'assegnazione e la gestione delle **Credenziali di autenticazione** per l'accesso ai dati personali degli **Incaricati del Trattamento,** su richiesta del **Responsabile del Trattamento**, avvalendosi del supporto tecnico dell'**incaricato della gestione e della manutenzione degli strumenti elettronici**, in conformità a quanto disposto dal **punto 3 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)**.
- Istruire gli incaricati del trattamento sull'uso delle **componenti riservata delle credenziali di autenticazione**, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia, in conformità a quanto disposto dal **punto 4 e dal punto 5 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)**.
- Assicurare che il **Codice per l'identificazione**, laddove sia stato già utilizzato, non sia assegnato ad altri **Incaricati del Trattamento**, neppure in tempi diversi, in conformità a quanto disposto dal **punto 6 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)**.

• Revocare le **Credenziali di autenticazione** per l'accesso ai dati degli **Incaricati del Trattamento** nel caso di mancato utilizzo per oltre 6 (sei) mesi, in conformità a quanto disposto dal **punto 7 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)**.
• Revocare tutte le **Credenziali di autenticazione** non utilizzate in caso di perdita della qualità che consentiva all'**Incaricato del Trattamento** l'accesso ai dati personali, in conformità a quanto disposto dal **punto 8 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)**.
• Impartire istruzioni agli **Incaricati del Trattamento** per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, in conformità a quanto disposto dal **punto 9 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003)**.

In caso di prolungata assenza o impedimento di un **Incaricato del Trattamento** che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, l'**Incaricato della custodia delle copie delle credenziali,** in accordo con il **Responsabile del Trattamento di dati personali** può assicurare la disponibilità di dati o strumenti elettronici operando secondo le seguenti istruzioni:

1. Utilizzando i diritti di "amministratore di sistema", può modificare in modo forzoso la **componente riservata delle credenziali di autenticazione** dell'**Incaricato del Trattamento dei dati personali** assente o impedito ad effettuare il trattamento.
2. Comunica la **componente riservata delle credenziali** di autenticazione così modificata ad un altro **Incaricato del Trattamento dei dati personali** designato dal **Responsabile del Trattamento di dati personali** il quale potrà utilizzarla solo temporaneamente.
3. Terminata l'assenza o l'impedimento dell'**Incaricato del Trattamento** che aveva reso indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, questo ultimo dovrà essere informato dell'intervento effettuato e dovrà modificare la propria componente riservata delle credenziali di autenticazione

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato della custodia delle copie delle credenziali**, ne assumerà tutte le responsabilità e funzioni.

In conformità a quanto disposto dai **punti 3, 4, 5, 6, 7, 8, 9 e 10 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. n. 196 del 30 giugno 2003), il Responsabile della sicurezza dei dati personali** nomina uno o

più soggetti **Incaricati della custodia delle copie delle credenziali** a cui è conferito il compito di autorizzare l'assegnazione e la gestione delle **Credenziali di autenticazione** per l'accesso ai dati gestiti con strumenti elettronici.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** deve essere effettuata con una lettera di incarico, deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve informare gli **Incaricati della custodia delle copie delle credenziali** della responsabilità che è stata loro affidata in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al D.Lgs. n. 196 del 30 giugno 2003)**.

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Incaricato della custodia delle copie delle credenziali**, una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** può essere revocata in qualsiasi momento dal **Responsabile della sicurezza dei dati personali** senza preavviso, ed essere affidata ad altro soggetto.

Incaricato delle copie di sicurezza delle banche dati

Bruno Giovanna Letizia
Pecoraro Valeriano

In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. n. 196 del 30 giugno 2003)** il **Responsabile della sicurezza dei dati personali**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dati**.

L'**Incaricato delle copie di sicurezza delle banche dati** è la persona fisica o la persona giuridica che ha il compito di sovrintendere alla esecuzione periodica delle copie di sicurezza delle **Banche di dati** personali gestite.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il **Responsabile della sicurezza dei dati personali** stabilisce, con il supporto tecnico dell'**Incaricato della gestione e della manutenzione degli strumenti elettronici** la periodicità con cui debbono essere effettuate le copie di sicurezza delle **Banche di dati** trattate.
I criteri debbono essere concordati con l'**Incaricato della gestione e della manutenzione degli strumenti elettronici** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. n. 196 del 30 giugno 2003)** la frequenza con cui debbono essere effettuate le copie dei dati personali non deve superare in nessun caso i 7 (sette) giorni.

In particolare per ogni **Banca di dati** debbono essere definite le seguenti specifiche:

- Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up".
- Il numero di "Copie di Back-Up" effettuate ogni volta.

- Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle "Copie di Back-Up".
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le "Copie di Back-Up".
- Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up".

E' compito degli **Incaricati delle copie di sicurezza delle banche dati**:

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal **Responsabile della sicurezza dei dati personali**.
- Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
- Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.
- Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
- Di segnalare tempestivamente all'**Incaricato della gestione e della manutenzione degli strumenti elettronici**, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato delle copie di sicurezza delle banche dati**, ne assumerà tutte le responsabilità e funzioni.

In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.Lgs. n. 196 del 30 giugno 2003)** il **Responsabile della sicurezza dei dati personali**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dati** a cui è conferito il compito di

effettuare periodicamente le copie di sicurezza delle Banche di dati gestite specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

Il **Responsabile della sicurezza dei dati personali** deve informare ciascun **Incaricato delle copie di sicurezza delle banche dati** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.Lgs. n. 196 del 30 giugno 2003)**.

La nomina di uno o più **Incaricati delle copie di sicurezza delle banche dati** deve essere effettuata con una lettera di incarico e deve essere controfirmata.

Copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Incaricato delle copie di sicurezza delle banche dati** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

Incaricati del Trattamento dei dati personali

Consiglieri dell'Ordine

INCARICATO TRATTAMENTO	MANSIONE
Corvo Fabio Salvatore	**Presidente**
Cannizzaro Nunzio	**Vice Presidente**
Cigna Rosario	**Segretario**
Contrafatto Paolo	**Tesoriere**
Notarsfefano Danilo	**Consigliere Delegato presso la Consulta Regionale degli Ordini Ingegneri di Sicilia**
Catalano Antonio	**Consigliere**
Marchese Egidio Elio Bruno	**Consigliere**
Samparisi Orazio	**Consigliere**
Saporito Francesco	**Consigliere**
Turturici Leonardo	**Consigliere**
Polizzi Alessandro	**Consigliere**

Dipendenti

INCARICATO TRATTAMENTO	MANSIONE
Bruno Giovanna Letizia	**Dipendente**
Pecoraro Valeriano	**Dipendente**

Commissione Parcelle

Raimondi Michele	**Di Vita Giuseppe**
Garro Giuseppe	**Garito Eduardo**
Dellutri Michele Pio	**Giuliana Sergio Maria**
Calì Salvatore	**Longo Gaetano Alfio**
Corvo Dario	**Pintavalle Totuccio**

Sberna Giuseppe	**Vaccaro Calogero**
Tumminelli Egidio Costantino	**Canalella Salvatore**
Andaloro Salvatore	**Falzone Valerio**
Caldarella Giuseppe	**Lo Porto Alfonso**
Giammusso Salvatore	**Milazzo Joseph**
Granvillano Ugo	**Samparisi Orazio**
Segura Francesco	**Cacioppo Salvatore**
Capizzello Roberto	**Latone Salvatore**
Lo Piano Ugo	**Palmeri Sebastiano**
Pizzardi Emilio	**Riccelli Davide**
Rinnone Salvatore	**Triberio Silvia**
Iudice Aurora A.	**La Ferrera Angelo**
Morello Carmelo	**Tedesco Maurizio G.**

Consiglio di Disciplina

INCARICATO TRATTAMENTO	**MANSIONE**
RAIMONDI Michele	**Presidente**
FRUTTIDORO Salvatore	**Segretario**
LOFORTE Vincenzo	**Componente**
SCARANTINO Costantino	**Componente**
MORSELLI Giuseppe Antonio	**Componente**
MARINO Maurizio	**Componente**
PILATO Cataldo	**Componente**
LA MANNA Biagino	**Componente**
LONGO Gaetano Alfio	**Componente**
LOMBARDO Rocco Orazio	**Componente**
BEVILACQUA Roberto Salvatore	**Componente**
SCHILLACI Giuseppe	**Componente Supplente**

LATONE Salvatore	**Componente Supplente**
GIULIANA Sergio Paolo	**Componente Supplente**
TANDURELLA Luigi Vladimiro	**Componente Supplente**
MISTRETTA Mario Carmelo	**Componente Supplente**
CARRUBBA Alessandro	**Componente Supplente**

In base a quanto stabilito dall'**Art. 30 del D.Lgs. n. 196 del 30 giugno 2003**, le operazioni di trattamento possono essere effettuate solo da **Incaricati del Trattamento** che operano sotto la diretta autorità del **Titolare del Trattamento** o, se designato, del **Responsabile del Trattamento di dati personali**, attenendosi alle istruzioni impartite.

In base a quanto definito dall'**Art. 4, punto 1, comma h) del D.Lgs. n. 196 del 30 giugno 2003**, gli "***Incaricati del Trattamento*** *sono persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal* ***Titolare del Trattamento*** *o, se designato, dal* ***Responsabile del Trattamento di dati personali***".

Per i **trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici,** gli **Incaricati del Trattamento dei dati personali** debbono osservare le seguenti disposizioni:

- Gli **Incaricati del Trattamento dei dati personali** sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.
- Il **Trattamento dei dati personali** deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli **interessati**.
- L'**Incaricato del Trattamento dei dati personali** deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.
- Ogni **Incaricato del Trattamento dei dati personali** è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

• Gli **Incaricati del Trattamento dei dati personali** che hanno ricevuto le **credenziali di autenticazione** per il trattamento dei dati personali, debbono conservare con la massima segretezza le **componenti riservate delle credenziali di autenticazione** (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.
• La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
• La **componente riservata delle credenziali di autenticazione** (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'incaricato.
• L'**Incaricato del Trattamento dei dati personali** deve modificare la **componente riservata delle credenziali di autenticazione** (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.
• In caso di trattamento di dati sensibili e di dati giudiziari la **componente riservata delle credenziali di autenticazione** (parola chiave) deve essere modificata almeno ogni tre mesi.
• Gli incaricati del trattamento non debbono **in nessun caso lasciare incustodito e accessibile lo strumento elettronico** durante una sessione di trattamento dei dati personali.

Per i **trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici** gli **Incaricati del Trattamento dei dati personali** debbono osservare le seguenti disposizioni:

• I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
• Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
• L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici , composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
• Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
• I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.

- Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.
- Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

La nomina di ciascun **Incaricato del Trattamento dei dati personali** deve essere effettuata dal **Titolare del Trattamento dei dati personali** con una **lettera di incarico** in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.
Copia della lettera di nomina firmata deve essere conservata a cura del **Responsabile del Trattamento di dati personali** in luogo sicuro.

Il **Responsabile del Trattamento di dati personali** deve informare ciascun **Incaricato del Trattamento dei dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto

stabilito dal **Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al D.Lgs. n. 196 del 30 giugno 2003)**.

Il **Responsabile del Trattamento di dati personali** deve consegnare a ciascun **Incaricato del Trattamento dei dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

Gli **Incaricati del Trattamento dei dati personali** devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli **Incaricati del Trattamento dei dati personali** deve essere assegnata una **credenziale di autenticazione**.

Agli **Incaricati del Trattamento dei dati personali** è prescritto di adottare le necessarie cautele per assicurare la segretezza della **componente riservata della credenziale di autenticazione** e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

La nomina dell'**Incaricato del Trattamento dei dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dell'**Incaricato del Trattamento dei Dati Personali** può essere revocata in qualsiasi momento dal **Responsabile del Trattamento di Dati personali** che gli ha affidato l'incarico, senza preavviso, ed eventualmente può essere affidata ad altro soggetto.

Responsabili Esterni per il Trattamento dei Dati

INCARICATO ESTERNO	PARTITA IVA	FINALITA'
Dott. Elisa Ingala	01221850850	CONSULENZA CONTABILE, FISCALE E DEL LAVORO
STUDIO CARDELLA - ING. ANGELO CARDELLA	01733680852	CONSULENZA SU MESSA A NORMA D. LGS. 196/03 CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Qualora il trattamento dei dati venisse affidato in parte o in toto a soggetti esterni alla struttura, la nomina di tali soggetti avverrà per iscritto mediante apposita lettera di incarico.
Sarà cura del Titolare conservare in luogo sicuro copia di tale lettera.
La scelta dei Responsabili del trattamento dati in esterno deve ricadere su soggetti che forniscano i requisiti di affidabilità previsti dal D. Lgs. 196/2003 (art. 29 comma 2).
Sarà compito del Responsabile esterno nominare gli incaricati e impartire loro la dovuta istruzione per garantire il trattamento e la conservazione dei dati in modo puntuale, lecito e sicuro.
Ogni trattamento di dati affidato a terzi verrà elencato nel presente capitolo nel quale sono individuate le sedi esterne nelle quali vengono fisicamente trattati e conservati i dati.
Al Titolare del trattamento spetta il compito di vigilare sull'operato del Responsabile Esterno affinché non vengano mai meno le misure minime di sicurezza dei dati.
Al momento dell'affidamento dell'incarico il **Responsabile Esterno del Trattamento dei Dati**, deve dichiarare per iscritto:

- Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali
- Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali
- Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.
- Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.
- Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

ANALISI DEI RISCHI

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio di dati di tipo informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi consiste nella:

- **individuazione di tutte le risorse del patrimonio informativo;**
- **identificazione delle minacce a cui tali risorse sono sottoposte;**
- **identificazione delle vulnerabilità;**
- **definizione delle relative contromisure.**

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- **DATI ANONIMI**, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- **DATI PERSONALI**,
  - **DATI PERSONALI SEMPLICI**, ovvero la classe di dati a rischio intermedio
  - **DATI PERSONALI SENSIBILI/GIUDIZIARI**, ovvero la classe di dati ad alto rischio;
  - **DATI PERSONALI SANITARI**, ovvero la classe di dati a rischio altissimo.

Individuazione delle risorse da proteggere

Le risorse da proteggere sono:

- personale;
- dati/informazioni;
- documenti cartacei;
- hardware;
- software;

Identificazione delle minacce a cui le risorse sono sottoposte

Di seguito sono elencate le minacce che e gli eventi pericolosi cui sono sottoposte le risorse relative al patrimonio dati informativo:

- Rischio d'area legato all'accesso non autorizzato nei locali
- Rischio d'area per furti di materiale cartaceo e/o elettronico
- Rischio d'area dovuto a mancata o non corretta manutenzione degli strumenti elettronici
- Rischio d'area dovuto ad interruzione di corrente
- Rischio d'area dovuto a linea elettrica instabile
- Rischio d'area per possibili eventi distruttivi
- Rischio d'area per possibili allagamenti / inondazioni
- Rischio legato a guasti o infiltrazioni nei servizi di comunicazione
- Rischio guasti tecnici per hardware, software supporti informatici
- Rischio legato ad uso illegale di software
- Rischio legato ad indirizzamento non corretto dei messaggi
- Rischio legato ad uso di software da parte di utenti non autorizzati
- Rischio legato a deterioramento dei supporti di memoria elettronici
- Rischio legato ad uso di software dannoso o pericoloso
- Rischio legato ad errori umani
- Rischio legato a uso non corretto delle risorse
- Rischio legato ad uso non autorizzato dei supporti di memoria
- Rischio legato ad errore del personale operativo

Identificazione delle vulnerabilità

- Mancanza di sistemi hardware di rimpiazzo
- Suscettibilità degli strumenti hardware a variazioni di temperatura e tensione
- Suscettibilità degli strumenti hardware ad umidità, polvere, sporcizia e a radiazioni elettromagnetiche
- Linea elettrica instabile
- Linee di comunicazione non protette
- Mancanza di identificazione / autorizzazione per l'accesso ai dati
- Permanenza di sessioni aperte senza utente
- Mancanza di copie di backup dei dati e dei programmi
- Incuria nella dismissione di supporti riscrivibili
- Gestione inadeguata della rete

Individuazione delle contromisure da attuare

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- **contromisure di carattere fisico;**
- **contromisure di carattere procedurale;**
- **contromisure di carattere elettronico/informatico.**

Contromisure di carattere fisico

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
- i locali ad accesso controllato sono all'interno di aree sotto la responsabilità del Amministratore di Sistema nominato;
- i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite a cura degli incaricati al trattamento;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità degli incaricati al trattamento;
- i locali sono provvisti di sistemi antincendio o estintore;
- per garantire la continuità elettrica gli elaboratori sono dotati di gruppi per assicurare la continuità elettrica

Contromisure di carattere procedurale

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- per l'ingresso ai locali ad accesso controllato è necessaria preventiva autorizzazione da parte del Responsabile del trattamento e successiva registrazione su apposito registro;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia dell'impianto antincendio o degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono

chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;

- i registri, contenenti dati comuni e particolari, durante l'orario di lavoro devono essere tenuti in e affidati al responsabile di turno. Al termine dell'orario di lavoro vengono depositati e successivamente raccolti da un incaricato del trattamento e conservati in luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio dell'orario di lavoro.
- il responsabile del trattamento dei dati è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del responsabile del trattamento dei dati che è chiuso a chiave, una chiave di riserva è mantenuta con le dovute cautele dalla ditta ;

Misure di carattere elettronico/informatico

Le misure di carattere elettronico/informatico adottate sono:

- presenza di gruppi di continuità elettrica per il server;
- installazione di un firewall per proteggere la rete dagli accessi indesiderati attraverso internet;
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows 2000 e XP;
- installazione di un sistema antivirus su tutte le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria;
- definizione delle regole per la gestione di strumenti elettronico / informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate;

Regole per la gestione di strumenti elettronico/informatico

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;

- le copie di backup realizzate sono conservate in armadio o cassetto chiuso a chiave
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screen-saver automatico dopo alcuni minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- Il fax si trova in locale ad accesso controllato e l'utilizzo è consentito unicamente agli incaricati del trattamento

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di aver adottato le misure minime di sicurezza previste dal disciplinare.

Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- disattivare gli ActiveX e il download dei file per gli utenti del browser Internet Explorer;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);

- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta(in quanto potrebbe essere falso e portare a un sito-truffa);
- consultare con periodicità mensile la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- non attivare le condivisioni dell'HD in scrittura.
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus;
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore di Sistema procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

- formattare l'Hard Disk,definire le partizioni e reinstallate il Sistema Operativo;
- installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

SEDI DEL TRATTAMENTO DEI DATI

Modalità di protezione dei locali e delle banche dati

In ottemperanza agli art. 31, 32, 33, 34, 35 e 36 del D. Lgs. 30/06/2003 n. 196, il presente DOCUMENTO prevede l'organizzazione di idonee misure di sicurezza da adottare volte a garantire la sicurezza dei dati.
La sicurezza dei dati si esplica nella loro diligente custodia al fine di prevenirne alterazioni, distruzione, diffusioni non autorizzate o trattamenti non conformi alle finalità della raccolta.
Il Responsabile del trattamento o, in mancanza, il Titolare appronteranno tutti i mezzi necessari per il perseguimento dei fini legati alla sicurezza dei dati, sfruttando anche le conoscenze acquisite in base al progresso tecnico.
Sono previste specifiche misure di sicurezza sia per quanto riguarda la custodia di archivi elettronici e non, che l'accesso ai locali ove i dati oggetto del trattamento fisicamente sono conservati.

Protezione dei locali e degli accessi

Durante il normale orario di lavoro il Responsabile del trattamento dati si occupa di verificare che le persone che accedono ai locali siano state preventivamente autorizzate all'accesso.
In questo capitolo sono inoltre illustrate le modalità di accesso alle singole sedi ed ai locali dove fisicamente vengono gestite le banche dati, sia nel caso di dati trattati con l'ausilio di strumenti elettronici che con altri strumenti.
Vengono altresì identificate, secondo quanto previsto al punto 19.4 dell'Allegato B, le misure adottate 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.

IDENTIFICAZIONE SEDE	SEDE CALTANISSETTA
UBICAZIONE SEDE	VIALE TRIESTE, 281 – 93100 - CALTANISSETTA
PROTEZIONI DI ACCESSO	• PORTA CON SERRATURA.
MODALITA' DI ACCESSO	CONSENTITO AL PUBBLICO.
ALTRE PROTEZIONI DELLA SEDE	ESTINTORE
NOMI UFFICIO	• DIREZIONE • SEGRETERIA 1 • SEGRETERIA 2 • SALA RIUNIONE • ARCHIVIO
MODALITA' ARCHIVIAZIONE DELLE BANCHE DATI ORDINARIE	SCAFFALI E CASSETTI
MODALITA' ARCHIVIAZIONE DELLE BANCHE DATI SENSIBILI/GIUDIZIARIE	ARMADI E CASSETTI CON SERRATURA.

IDENTIFICAZIONE SEDE	SEDE GELA
UBICAZIONE SEDE	PIAZZA SAN FRANCESCO, 2 – 93012 – GELA
PROTEZIONI DI ACCESSO	• PORTA CON SERRATURA.
MODALITA' DI ACCESSO	CONSENTITO AL PUBBLICO.
ALTRE PROTEZIONI DELLA SEDE	ESTINTORE
NOMI UFFICIO	• DIREZIONE • SALA RIUNIONE
MODALITA' ARCHIVIAZIONE DELLE BANCHE DATI ORDINARIE	SCAFFALI E CASSETTI
MODALITA' ARCHIVIAZIONE DELLE BANCHE DATI SENSIBILI/GIUDIZIARIE	ARMADI E CASSETTI CON SERRATURA.

TRATTAMENTI DEI DATI PERSONALI

Modalità generali di Trattamento

Al Responsabile del Trattamento dei dati è affidato il compito di redigere e di aggiornare l'elenco dei trattamenti effettuati sui dati personali come descritto nel presente capitolo.

Trattamento dati in formato cartaceo

Modalità di accesso ai dati

Gli incaricati devono operare sui dati osservando scrupolosamente i limiti e relativamente alle mansioni loro affidate ed alle finalità di trattamento perseguite.

Modalità di consultazione

La consultazione dei dati avviene in maniera riservata assicurandosi che nessun altro, ad esclusione dell'incaricato, possa prendere visione del documento in trattamento.

Custodia e responsabilità del supporto

Sarà cura dell'incaricato assicurare che i dati personali affidatigli non siano consultati da soggetti non autorizzati. Durante una sessione di trattamento l'incaricato ha l'obbligo di non lasciare incustoditi i dati personali e di riporli alla fine del trattamento.

Divieto di copia e riproduzione

E' fatto divieto all'incaricato di fare delle copie o riprodurre i documenti trattati. Fatto salvo il caso in cui l'oggetto del trattamento non sia esplicitamente la copia o la riproduzione al fine di garantire i diritti dell'interessato, oppure sia stato straordinariamente autorizzato dal titolare o dal responsabile del trattamento.

Trattamento dati in formato elettronico

Così come previsto dall'Allegato B al D.Lgs. 196/2003, il trattamento dei dati personali con strumenti elettronici è consentito solo agli incaricati dotati di credenziali di autenticazione che consentono il superamento di una procedura di autenticazione.

Il Responsabile del Trattamento (o in mancanza, il Titolare), in accordo con gli Amministratori di sistema, definisce le modalità di assegnazione delle credenziali di autenticazione agli incaricati del Trattamento. Le credenziali possono consistere nell'assegnazione di User ID e password o nell'utilizzo di dispositivi associati ad un codice identificativo o anche ad una caratteristica biometrica.

Ad ogni soggetto autorizzato all'accesso alle banche dati possono essere assegnate anche più credenziali per l'autenticazione in base alle esigenze organizzative o al numero di banche dati gestite.

DESCRIZIONE BANCA DATI
ARCHIVIO COMPENSI DIPENDENTI
Archivio contratti forniture ed assicurazioni varie con riferimenti a fornitori di servizi.
Archivio documentazione contabile e fiscale contente dati iscritti, fornitori e dipendenti.
Archivio documentazione dipendenti contenente lettere di incarico, certificati medici libretti di lavoro, e documentazione varia.
Archivio documentazione per la gestione dei conti correnti bancari.
Archivio fatture acquisti con riferimenti a fornitori
Archivio ricevute emesse agli iscritti
Archivio storico di ricevute emesse agli iscritti
Archivio primanota contabile contenente dati clienti, fornitori e dipendenti
LIBRO PRESENZE ED INFORTUNI DIPENDENTI
ARCHIVIO DOCUMENTAZIONE PRIVACY CON RIFERIMENTO ISCRITTI
RUBRICA TELEFONICA NUMERI DI UTILITA'
ARCHIVIO INFORMATIVE PRIVACY FIRMATE
ARCHIVIO CORRISPONDENZA ENTRATA E USCITA E REGISTRO DI PROTOCOLLO
ARCHIVIO STORICO DI CORRISPONDENZA ENTRATA E USCITA E REGISTRO DI PROTOCOLLO
ARCHIVIO ISCRITTI ALL'ALBO CARTELLE PERSONALI
ARCHIVIO DELLE PARCELLE E DOCUMENTAZIONE VARIA E ATTO APPROVAZIONE
CARTELLA PRATICHE LEGALI
ARCHIVIO STORICO VERBALI ORDINI, REGISTRI
ARCHIVIO CIRCOLARI
ARCHIVIO SOLLECITI DI PAGAMENTI PER ISCRITTI ALL'ORDINE
INFORMAZIONI DI UTILITA' SUGLI ISCRITTI
ARCHIVIO COMUNICAZIONI AD CONSIGLIERI E COMMISSIONI VARIE
DOCUMENTAZIONE SULLA CARTELLA PERSONALE: DOMANDA DI ISCRIZIONE, CERTIFICATO DI NASCITA, CERTIFICATO DI CITTADINANZA, CERTIFICATO DI RESIDENZA, CERTIFICATO GENERALE DEL CASELLARIO GIUDIZIALE, CERTIFICATO DI LAUREA CERTIFICARO DELL'ESAME DI STATRO, NUMERO DEL CODICE FISCALE ATTRIBUITO, RICEVUTA DELLA TASSA DI CONSESSIONE GOVERNATIVA, RICEVUTA DI VERSAMENTO, N. 2 DI FOTOGRAFIE.
Cartella Documenti Su PC

ELENCO DEI TRATTAMENTI DEI DATI PERSONALI AFFIDATI A CIASCUN INCARICATO

MODALITA'

LEGENDA PERMESSI		
A – Acquisizione	I – Inserimento	M – Modifica
S – Scrittura	L – Lettura	C - Cancellazione

DESCRIZIONE DEL TRATTAMENTO	**PERMESSI**						
Bruno Giovanna Letizia	**TUTTI**	**A**	**I**	**M**	**S**	**L**	**C**
ARCHIVIO COMPENSI DIPENDENTI	**X**						
Archivio contratti forniture ed assicurazioni varie con riferimenti a fornitori di servizi.	**X**						
Archivio documentazione contabile e fiscale contente dati iscritti, fornitori e dipendenti.	**X**						
Archivio documentazione dipendenti contenente lettere di incarico, certificati medici libretti di lavoro, e documentazione varia.	**X**						
Archivio documentazione per la gestione dei conti correnti bancari.	**X**						
Archivio fatture acquisti con riferimenti a fornitori	**X**						
Archivio ricevute emesse agli iscritti	**X**						
Archivio storico di ricevute emesse agli iscritti	**X**						
Archivio primanota contabile contenente dati clienti, fornitori e dipendenti	**X**						
LIBRO PRESENZE ED INFORTUNI DIPENDENTI	**X**						
ARCHIVIO DOCUMENTAZIONE PRIVACY CON RIFERIMENTO ISCRITTI	**X**						
RUBRICA TELEFONICA NUMERI DI UTILITA'	**X**						
ARCHIVIO INFORMATIVE PRIVACY FIRMATE	**X**						
ARCHIVIO CORRISPONDENZA ENTRATA E USCITA E REGISTRO DI PROTOCOLLO	**X**						
ARCHIVIO STORICO DI CORRISPONDENZA ENTRATA E USCITA E REGISTRO DI PROTOCOLLO	**X**						
ARCHIVIO ISCRITTI ALL'ALBO CARTELLE PERSONALI	**X**						
ARCHIVIO DELLE PARCELLE E DOCUMENTAZIONE VARIA E ATTO APPROVAZIONE	**X**						
CARTELLA PRATICHE LEGALI	**X**						
ARCHIVIO STORICO VERBALI ORDINI, REGISTRI	**X**						
ARCHIVIO CIRCOLARI	**X**						
ARCHIVIO SOLLECITI DI PAGAMENTI PER ISCRITTI ALL'ORDINE	**X**						
INFORMAZIONI DI UTILITA' SUGLI ISCRITTI	**X**						

ARCHIVIO COMUNICAZIONI AD CONSIGLIERI E COMMISSIONI VARIE	**X**						
DOCUMENTAZIONE SULLA CARTELLA PERSONALE: DOMANDA DI ISCRIZIONE, CERTIFICATO DI NASCITA, CERTIFICATO DI CITTADINANZA, CERTIFICATO DI RESIDENZA, CERTIFICATO GENERALE DEL CASELLARIO GIUDIZIALE, CERTIFICATO DI LAUREA CERTIFICARO DELL'ESAME DI STATRO, NUMERO DEL CODICE FISCALE ATTRIBUITO, RICEVUTA DELLA TASSA DI CONSESSIONE GOVERNATIVA, RICEVUTA DI VERSAMENTO, N. 2 DI FOTOGRAFIE.	**X**						
Cartella Documenti Su PC segreteria 1	**X**						

DESCRIZIONE DEL TRATTAMENTO	**PERMESSI**						
Pecoraro Valeriano	**TUTTI**	**A**	**I**	**M**	**S**	**L**	**C**
Archivio contratti forniture ed assicurazioni varie con riferimenti a fornitori di servizi.	**X**						
Archivio fatture acquisti con riferimenti a fornitori						**X**	
Rapporto delle presenze			**X**	**X**			
ARCHIVIO DOCUMENTAZIONE PRIVACY CON RIFERIMENTO ISCRITTI	**X**						
RUBRICA TELEFONICA NUMERI DI UTILITA'	**X**						
ARCHIVIO INFORMATIVE PRIVACY FIRMATE	**X**						
ARCHIVIO ISCRITTI ALL'ALBO CARTELLE PERSONALI	**X**						
ARCHIVIO STORICO VERBALI ORDINI, REGISTRI	**X**						
REGISTRI RITIRI STRUMENTAZIONE	**X**						
ARCHIVIO CIRCOLARI	**X**						
REGISTRAZIONI AUDIO DI CORSI EFFETTUATI	**X**						
INFORMAZIONI DI UTILITA' SUGLI ISCRITTI	**X**						
Cartella Documenti Su PC segreteria 2	**X**						
Gestione Newsletter dell'Ordine	**X**						
Aggiornamento tramite CMS del sito dell'Ordine	**X**						

DESCRIZIONE DEL TRATTAMENTO	**PERMESSI**						
Presidente e Consiglio Ordine	**TUTTI**	**A**	**I**	**M**	**S**	**L**	**C**
ARCHIVIO COMPENSI DIPENDENTI	**X**						
Archivio contratti forniture ed assicurazioni varie con riferimenti a fornitori di servizi.	**X**						
Archivio documentazione contabile e fiscale in fase di registrazione contenente dati clienti e fornitori e dipendenti.	**X**						
Archivio documentazione dipendenti contenente lettere di incarico, certificati medici libretti di lavoro, e documentazione varia.	**X**						

Archivio documentazione per la gestione dei conti correnti bancari.	**X**						
Archivio fatture acquisti con riferimenti a fornitori	**X**						
Archivio ricevute emesse agli iscritti	**X**						
Archivio storico di ricevute emesse agli iscritti	**X**						
Archivio primanota contabile contenente dati clienti, fornitori e dipendenti	**X**						
LIBRO PRESENZE ED INFORTUNI DIPENDENTI	**X**						
ARCHIVIO DOCUMENTAZIONE PRIVACY CON RIFERIMENTO ISCRITTI	**X**						
RUBRICA TELEFONICA NUMERI DI UTILITA'	**X**						
ARCHIVIO INFORMATIVE PRIVACY FIRMATE	**X**						
ARCHIVIO CORRISPONDENZA ENTRATA E USCITA E REGISTRO DI PROTOCOLLO	**X**						
ARCHIVIO STORICO DI CORRISPONDENZA ENTRATA E USCITA E REGISTRO DI PROTOCOLLO	**X**						
ARCHIVIO ISCRITTI ALL'ALBO CARTELLE PERSONALI	**X**						
ARCHIVIO DELLE PARCELLE E DOCUMENTAZIONE VARIA E ATTO APPROVAZIONE	**X**						
CARTELLA PRATICHE LEGALI	**X**						
ARCHIVIO STORICO VERBALI ORDINI, REGISTRI	**X**						
REGISTRI RITIRI STRUMENTAZIONE	**X**						
ARCHIVIO CIRCOLARI	**X**						
REGISTRAZIONI AUDIO DI CORSI EFFETTUATI	**X**						
ARCHIVIO SOLLECITI DI PAGAMENTI PER ISCRITTI ALL'ORDINE	**X**						
INFORMAZIONI DI UTILITA' SUGLI ISCRITTI	**X**						
ARCHIVIO COMUNICAZIONI AD CONSIGLIERI E COMMISSIONI VARIE	**X**						
DOCUMENTAZIONE SULLA CARTELLA PERSONALE: DOMANDA DI ISCRIZIONE, CERTIFICATO DI NASCITA, CERTIFICATO DI CITTADINANZA, CERTIFICATO DI RESIDENZA, CERTIFICATO GENERALE DEL CASELLARIO GIUDIZIALE, CERTIFICATO DI LAUREA CERTIFICARO DELL'ESAME DI STATRO, NUMERO DEL CODICE FISCALE ATTRIBUITO, RICEVUTA DELLA TASSA DI CONSESSIONE GOVERNATIVA, RICEVUTA DI VERSAMENTO, N. 2 DI FOTOGRAFIE.	**X**						
Cartella Documenti Su PC segreteria 1	**X**						

DESCRIZIONE DEL TRATTAMENTO	**PERMESSI**						
Commissione Parcelle	**TUTTI**	**A**	**I**	**M**	**S**	**L**	**C**
Atti storici approvazione parcelle	**X**						
Parcelle e documentazione varia e atto approvazione	**X**						

DESCRIZIONE DEL TRATTAMENTO	PERMESSI						
Consiglio di Disciplina	**TUTTI**	**A**	**I**	**M**	**S**	**L**	**C**
Atti e Documentazione relativa alla valutazione della Disciplina degli Iscritti	**X**						

ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI

Protezione dei dati

Al fine di proteggere le Banche Dati da intrusioni informatiche di soggetti o programmi non autorizzati al trattamento, sono utilizzati appositi strumenti software.

Protezione dei supporti rimovibili

I supporti rimovibili sono affidati in custodia all'incaricato del trattamento. Il responsabile del Trattamento dati si assicurerà che i supporti rimovibili non saranno condotti al di fuori dei locali in cui i dati sono trattati.

Distruzione dei supporti rimovibili

I supporti rimovibili che contengono dati non più utilizzati sono distrutti cancellando i dati in essi contenuti ove questo sia possibile. Nel caso di supporti non riscrivibili questi sono distrutti fisicamente.

Dati relativi allo stato di salute e la vita sessuale

In applicazione dell'Art 22 c.6 D.Lgs. 196/2003 e dell'allegato B punto 24, i dati relativi allo stato di salute e alla vita sessuale dell'interessato sono trattati in forma anonima prevedendo la separazione dei dati sensibili dai dati identificativi. Qualora si rendesse

necessario l'individuazione dell'interessato, questa avviene in maniera indiretta recuperando dai dati identificativi il codice identificativo univoco e ricercando i dati sensibili che corrispondono a detto codice univoco.
A cura dell'incaricato al Trattamento i dati relativi all'identità genetica sono trattati esclusivamente all'interno dei locali assegnati alla banca dati.
Il trasferimento dei dati all'esterno dei locali riservati al loro trattamento avviene in contenitori muniti di apposita serratura. I dati elettronici sono trasportati dopo aver subito un apposito trattamento di cifratura.

REGOLE PER LA GESTIONE DELLE PASSWORD

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale.
User-id e password iniziali sono assegnati, dal custode delle password.
User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.
La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.
Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password;
Il custode delle password provvederà a sostituire la precedente busta con quest'ultima.
Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.
Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.
In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.

Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:
le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;

per la definizione/gestione della password devono essere rispettate le seguenti regole:

- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere lo user-id come parte della password;
- al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
- la nuova password non deve essere simile alla password precedente;
- la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
- la password termina dopo sei mesi di inattività;
- la password è segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;
- l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia

INVENTARIO E CARATTERISTICHE DEGLI ELABORATORI ELETTRONICI

MODALITA' OPERATIVE

Il Responsabile del Trattamento o il Titolare incaricano l'Amministratore del Sistema ad approntare tutte le misure di sicurezza idonee a prevenire e ridurre infezioni da Virus informatici o da intrusioni non autorizzate nel sistema.

L'amministratore provvederà a dettagliare nel seguente capitolo tutte le misure adottate compresi l'utilizzo di appositi programmi Antivirus, Firewall e qualsiasi ulteriore soluzione informatica che ritenesse opportuna per diminuire la vulnerabilità del sistema.

E' anche compito dell'Amministratore di Sistema pianificare il lavoro relativo all'installazione degli aggiornamenti messi a disposizione delle case produttrici di software per correggere i difetti dei programmi o dei sistemi operativi utilizzati. L'amministratore può prevedere anche che il periodico aggiornamento dei programmi utilizzati per garantire la sicurezza informatica avvenga in un arco di tempo inferiore a quanto previsto dal D.Lgs. 30/06/2003 n. 196.

Tutte le misure di sicurezza previste dall'amministratore di sistema dovranno essere periodicamente valutate per adattare la procedura all'evoluzione tecnologica.

L'amministratore di sistema dovrà provvedere ad istruire adeguatamente eventuali incaricati al trattamento relativamente alle misure adottate, e descritte nel seguente capitolo.

In caso di infezione del sistema da parte di Virus informatici, l'amministratore del sistema dovrà tempestivamente adottare tutte le misure idonee per isolare il sistema ed evitare che il danno venga esteso ad altri elaboratori; dovrà quindi individuare le cause di tale infezione e provvedere a rimuoverle.

SEDE CALTANISSETTA

NOME ELABORATORE	PC SEGRETERIA 1 - BRUNO
SISTEMA OPERATIVO	WINDOWS
ANTIVIRUS	PRESENTE
CONNETTIVITA'	ADSL
FIREWALL	PRESENTE
GRUPPO CONTINUITA'	PRESENTE
PASSWORD	ACCESSO E SCREEN SAVER PRESENTI
DISPOSITIVO BACKUP	MASTERIZZATORE / HARD DISK ESTERNO

NOME ELABORATORE	PC PRESIDENTE ORDINE E CONSIGLIO ORDINE
SISTEMA OPERATIVO	WINDOWS
ANTIVIRUS	PRESENTE
CONNETTIVITA'	ADSL
FIREWALL	PRESENTE
GRUPPO CONTINUITA'	PRESENTE
PASSWORD	ACCESSO E SCREEN SAVER PRESENTI
DISPOSITIVO BACKUP	MASTERIZZATORE / HARD DISK ESTERNO

NOME ELABORATORE	NOTEBOOK 1 – PECORARO
SISTEMA OPERATIVO	WINDOWS
ANTIVIRUS	PRESENTE
CONNETTIVITA'	ADSL
FIREWALL	PRESENTE
GRUPPO CONTINUITA'	PRESENTE
PASSWORD	ACCESSO E SCREEN SAVER PRESENTI
DISPOSITIVO BACKUP	MASTERIZZATORE / HARD DISK ESTERNO

NOME ELABORATORE	NOTEBOOK 2 – COMMISSIONE PARCELLE CALTANISSETTA
SISTEMA OPERATIVO	WINDOWS
ANTIVIRUS	PRESENTE
CONNETTIVITA'	ADSL
FIREWALL	PRESENTE
GRUPPO CONTINUITA'	PRESENTE
PASSWORD	ACCESSO E SCREEN SAVER PRESENTI
DISPOSITIVO BACKUP	MASTERIZZATORE / HARD DISK ESTERNO

NOME ELABORATORE	NOTEBOOK 3 – COMMISSIONE PARCELLE GELA
SISTEMA OPERATIVO	WINDOWS
ANTIVIRUS	PRESENTE
CONNETTIVITA'	ADSL
FIREWALL	PRESENTE
GRUPPO CONTINUITA'	PRESENTE
PASSWORD	ACCESSO E SCREEN SAVER PRESENTI
DISPOSITIVO BACKUP	MASTERIZZATORE / HARD DISK ESTERNO

PIANI DI FORMAZIONE DEGLI INCARICATI

MODALITA' OPERATIVE

Al Responsabile (o in mancanza al Titolare), come descritto nei punti 19.6 e 27 dell'Allegato B, spetta il compito di provvedere all'opportuna formazione di tutti gli incaricati al trattamento dei dati al fine di:

- garantire il massimo rispetto delle procedure elencate nel presente DOCUMENTO
- rendere edotto il personale sui rischi che incombono sui dati
- informare il personale sulle responsabilità che ne derivano

Il Responsabile (o in mancanza il Titolare) valuterà opportunamente il livello di preparazione dei singoli addetti in merito alle procedure (informatiche e non) utilizzate per il trattamento e la custodia dei dati; eventuali lacune saranno colmate con appositi interventi formativi volti a rendere i soggetti interessati idonei a svolgere gli incarichi loro assegnati.

Il Titolare o il Responsabile, con cadenza almeno annuale, provvederanno a verificare le esigenze di formazione del personale in base all'esperienza acquisita, al progresso tecnologico o al cambiamento di mansioni.

Formazione da Impartire

Di seguito sono elencate tutte le necessità di formazione dei soggetti nominati quali Incaricati del trattamento dati.

Custodia dello strumento elettronico

Durante una sessione di trattamento di dati personali con apposito corso formativo, organizzato a cura del Responsabile del Trattamento, viene sensibilizzato il personale incaricato al trattamento e alla custodia dello strumento elettronico in particolare durante una sessione di trattamento

Rischi incombenti sui dati

Apposito corso formativo organizzato dal Responsabile del illustra i capitoli AR che disciplinano i rischi incombenti sui dati. Viene istruito il personale incaricato del trattamento all'utilizzo corretto degli applicativi che consentono l'acceso ai dati ed è

sensibilizzato ad adoperare la diligenza del 'buon padre di famiglia' per i rischi la cui individuazione richiede una specifica conoscenza tecnica.

Misure preventive di eventi dannosi

Con apposito corso viene sensibilizzato il personale incaricato del trattamento a non attuare azioni che possano danneggiare gli elaboratori elettronici ed i dati in essi contenuti. Il personale incaricato è ammonito sulle responsabilità a loro carico dettate dalla normativa vigente ed è stato sensibilizzato sulle misure minime di sicurezza da adottare.

Conoscenza delle norme e delle parti rilevanti in relazione al trattamento dei dati ed al settore di attività aziendale

In un corso oculatamente organizzato viene data lettura dell'allegato B del D.Lgs. 196/2003 e del Documento di Programmazione sulla Sicurezza dei dati personali. Si rapporta la norma alle esigenze della nostra attività aziendale chiarendo contestualmente i dubbi che il personale incaricato del trattamento ha posto. E' resa disponibile per la consultazione a tutti i soggetti elencati una copia del D.Lgs 196/2003 e, su richiesta, è possibile prendere visione del DOCUMENTO.

Custodia ed uso dei supporti rimovibili contenenti dati personali,sensibili o giudiziari.

Si invita il personale incaricato del trattamento a non lasciare incustoditi i supporti rimovibili contenenti dati personali, di non condurre supporti rimovibili all'esterno degli uffici in cui il trattamento è effettuato. Infine è fatto assoluto divieto di condurre dati sensibili o giudiziari all'esterno dei locali in cui si effettua il trattamento.

Controllo e custodia per l'intero ciclo di trattamento di dati senza supporto di strumenti elettronici.

Le procedure per il controllo, la custodia ed il trattamento di dati personali senza l'ausilio di strumenti elettronici sono descritti nel presente DOCUMENTO.
A cura del responsabile viene organizzato apposito corso formativo che coinvolge tutti gli incaricati in cui è illustrato il documento sopramenzionato e nel quale si chiariscono ulteriori quesiti posti dagli incaricati.

FIRME

Il presente documento **nell'ambito dell'aggiornamento con cadenza almeno annuale** della lista degli incaricati, degli addetti alla gestione e manutenzione degli strumenti elettronici e dell'individuazione dei trattamenti consentiti agli incaricati è da considerarsi in ottemperanza a quando disciplinato dall'ALLEGATO B del D. Lgs. 196/06 e successive modifiche e integrazioni.

21 Ottobre 2016

Titolare del Trattamento:

_____

(**Ordine degli Ingegneri della Provincia di Caltanissetta**)

Responsabile del Trattamento:

_____

(Bruno Giovanna Letizia)