AUTORITA' D'AMBITO A.T.O. n° 3 MESSINA
Servizio Idrico Integrato
Segreteria Tecnico Operativa

Repubblica Italiana Regione Siciliana Provincia Regionale

DETERMINAZIONE DIRIGENZIALE N° **94** DEL **11.12.2012**

Oggetto: Approvazione Documento Programmatico sulla sicurezza D.Lgs.196/2003 e s.m.i. - Aggiornamento 10 Dicembre 2012

IL DIRIGENTE RESPONSABILE DELLA S.T.O.

PREMESSO che l'art. 4 del Regolamento di Organizzazione e funzionamento della S.T.O. dell'A.T.O. 3 S.I.I. di MESSINA, conferisce al Dirigente Responsabile della stessa Segreteria, piena autonomia amministrativa, tecnica e contabile-finanziaria, nonché i poteri e le discrezionalità necessari per l'esercizio delle funzioni proprie della S.T.O. ed in piena autonomia, lo svolgimento delle attività gestionali connesse;

DATO ATTO che con determina n° **62** del 14/09/2010 sono state definite le regole per l'organizzazione degli uffici e dei servizi; nella stessa la Responsabilità dei Sistemi Informatici veniva accorpata alla Segreteria del Direttore Responsabile;

CHE con determina n° **77** del 23/09/2010 sono state attribuite al personale le relative aree professionali;

CHE con determina n° **78** del 23/09/2010 sono stati nominati i Responsabili delle Unità Organizzative; in particolare veniva nominato Responsabile dell'Area Amministrativa il sig. Caminiti Antonio e confermato Responsabile UO Area Tecnica l'ing. Torre Salvatore;

CHE con determina n° **99** del 13/10/2010 sono stati attribuiti compiti e funzioni alle Unità Organizzative attribuendo alla U.O. "Segreteria Direttore Responsabile" anche le funzioni di "Sistemi informatici ed elaborazione dati";

CHE con nota n° **92755** del 26/11/2010, nella veste di F.R.U.O. Pianificazione e Controllo e Responsabile della Rete, l'Ing.Torre Salvatore ha relazionato al Dirigente Responsabile della S.T.O. lo stato di consistenza e trasmesso i relativi atti;

CHE con determina n° **186** del 29/12/2010 è stato assegnata al Dott.Vincenzo Palana la responsabilità dell'U.O. "Segreteria Direttore Responsabile" nella qualità di Funzionario Direttivo ctg.D;

CHE con determina n° **4** del 17/01/2011 è stato conferito al Dott.Vincenzo Palana l'incarico di Responsabile dei Sistemi informatici della Segreteria Tecnico Operativa dell'A.T.O. n.3 di Messina;

CHE con determina n° **46** del 17/03/2011 è stata conferita al Dott.Vincenzo Palana l'incarico di P.O. per l'Area Amministrativa conglobando l'U.O. Sistemi informatici della Segreteria Tecnico Operativa dell'A.T.O. n.3 di Messina;

CHE con determina n° **49** del 21/03/2011 è stata incaricata la CIME per l'assistenza tecnico organizzativa di supporto per la riorganizzazione della rete informatica e la redazione del Documento Programmatico Sicurezza (D.P.S.) della Segreteria Tecnico Operativa dell'A.T.O. n.3 di Messina;

CONSIDERATO che pertanto necessita approvare l'aggiornamento del Documento Programmatico sulla Sicurezza (D.P.S.) previsto in materia di protezione di dati personali dal D.Lgs.196/2003;

CHE l'art. 31 del D.lgs. 196/03 "Codice in materia di protezione dati personali" stabilisce che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, 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;

CHE l'art. 33 del medesimo Decreto, precisa che i Titolari del trattamento sono tenuti ad adottare le misure minime ivi indicate;

CHE l'insieme delle misure tecniche, informatiche, organizzative per attivare il livello minimo di protezione richiesto dal citato art. 33 e' stato definito dagli artt. 34-35-36 e dall'allegato B del medesimo testo normativo;

RILEVATO che l'art. 34 del D.lgs. 196/03 prevede che per il trattamento dei dati personali effettuato con strumenti elettronici ci si attenga alle misure stabilite nell'allegato B, e precisa, alla lettera g), l'obbligo della tenuta di un aggiornato Documento Programmatico sulla Sicurezza;

VISTO in particolare il punto n. 19 dell'allegato B del menzionato Decreto Legislativo, Il quale prevede che il Titolare di trattamenti di dati Sensibili o Giudiziari, entro il 31 marzo di ogni anno, rediga e predisponga un apposito "DOCUMENTO PROGRAMMATICO SULLA SICUREZZA";

CHE pertanto si rende necessario approvare l'allegato D.P.S. – Aggiornamento 10/12/2012 - redatto in base alle disposizioni del Disciplinare tecnico in materia di protezione dei dati personali (art.34 all.B regola 19 del D.Lgs 196 del 30.06.2003 e delle Linee guida fornite dal Garante per la Privacy del giugno 2004;

CONSIDERATO che l'aggiornamento dei nominativi degli Amministratori di sistema, i relativi ambiti di operatività, i loro profili autorizzativi e la predisposizione di un sistema centralizzato per la gestione dei log in grado di raccogliere e storicizzare le informazioni relative agli utenti, sono requisiti minimi richiesti dal Garante e da integrare all'interno del più generale Documento Programmatico sulla Sicurezza dei Dati;

CHE il Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al T.U. 196 del 2003) stabilisce che deve essere riferito, nella relazione accompagnatoria del bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del Documento Programmatico sulla Sicurezza dei Dati;

QUANTO SOPRA PREMESSO

DETERMINA

APPROVARE in base alla narrativa che precede e che qui si intende integralmente riportata, l'allegato Documento Programmatico sulla Sicurezza per l'adozione delle misure di sicurezza nel trattamento dei dati personali (D.P.S.);

DARE ATTO che il D.P.S. – Aggiornamento 10/12/2012 - è depositato agli atti presso l'Area Amministrativa di questa Segreteria Tecnico Operativa al prot.2676 dell'11/12/2012.

DARE ATTO che la presente determinazione non comporta impegno di spesa.

TRASMETTERE copia per la pubblicazione all'Albo Pretorio della Provincia Regionale di Messina.

Il Dirigente Responsabile della S.T.O.
Avv. Giuseppe Santalco

AUTORITA' D'AMBITO A.T.O. 3
MESSINA

Via S.Paolo ex IAI
MESSINA (ME)
Partita IVA: 97072340835

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto in base alle disposizioni del

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

del CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (art.34 e Allegato B, regola 19, del d.lgs. 30 giugno 2003, 196)

e delle LINEE GUIDA fornite dal Garante per la Privacy del 11 giugno 2004

Aggiornamento 10 Dicembre 2012

1. SCOPO

Lo scopo del presente Documento Programmatico sulla Sicurezza è di delineare il quadro delle misure minime di sicurezza che debbono essere adottate in via preventiva da tutti coloro che trattano dati personali comuni, sensibili o giudiziari, conformemente a quanto previsto dal D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) e dal Disciplinare Tecnico, Allegato B al predetto Codice.

In conformità con le previsioni di cui all'articolo 31 del Codice, scopo del presente Documento Programmatico sulla Sicurezza è di ridurre al minimo 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, intendendosi per misure di sicurezza il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di cui sopra.

Il presente documento ha validità annuale e potrà essere aggiornato nel caso in cui le informazioni in esso contenute non siano più rispondenti all'effettiva organizzazione del trattamento dei dati. In ogni caso, il Titolare del trattamento, entro il 31 marzo di ogni anno, dovrà verificarlo ed eventualmente aggiornarlo.

Titolare del trattamento dei dati personali, con il compito di vigilare affinché i Responsabili del trattamento rispettino le sue istruzioni e ottemperino alle previsioni del Codice in materia di protezione dei dati personali è:

- AUTORITA' D'AMBITO A.T.O. 3 MESSINA

Via S.Paolo ex IAI
MESSINA (ME)
Partita IVA: 97072340835

2. CAMPO DI APPLICAZIONE

Il Documento Programmatico Sulla Sicurezza riguarda il trattamento di tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

e si applica al trattamento di tutti i dati personali effettuato per mezzo di:

- strumenti elettronici di elaborazione
- altri strumenti di elaborazione

Esso deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

3. RIFERIMENTI NORMATIVI

- D. Lgs. nr. 196/2003 (Codice in materia di protezione dei dati personali)
- Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B al D. Lgs. n. 196/2003)

4. 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.

5. ELENCO DEI TRATTAMENTI DI DATI PERSONALI (REGOLA 19.1)

001 - Archivio clienti, fornitori, procedure contabili

Finalità perseguite: Gestione della clientela; Gestione dei fornitori; Trattamento economico e giuridico del personale; Formazione professionale per il personale; Adempimento di obblighi fiscali o contabili; Programmazione delle attività; Gestione del patrimonio mobiliare e immobiliare; Gestione del contenzioso; Servizi di controllo interno (sicurezza); Servizi di controllo interno (produttività); Servizi di controllo interno (qualità dei sevizi); Servizi di controllo interno (integrità del patrimonio)
Categorie di dati trattati: Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati contabili
Categorie di soggetti interessati: Clienti; Fornitori; Dipendenti; Collaboratori; Altri soggetti

Natura dei dati trattati: PERSONALI
Modalità del trattamento: INTERNO; ELETTRONICO E CARTACEO; NON CIFRATO.

Luogo di ubicazione della banca dati:
Stanza Server
Indirizzo: Via S.Paolo ex IAI - MESSINA (ME)
Attività svolta: area CED dove sono collocati i 3 Server, protetta da chiave, installato climatizzatore in uso nel perido estivo
Tipologia di accesso: Non consentito al pubblico
Tipologia di chiusura: Con serratura
Impianto di allarme: Non installato
Impianto anticendio: Non installato
Soggetti autorizzati all'ingresso nei locali: Palana Vincenzo; Sarlo Domenico; Torre Salvatore

Strumenti elettronici utilizzati: SERVER G6
Il Server G6 è il principale contenitore di Dati, e funge da Server di Backup dei Server G4 e G3. Il piano di backup schedulato è descritto in dettaglio nell' Allegato Backup

Caratteristiche dello strumento: Collegamento a internet; Collegamento a rete locale (LAN); Disco removibile; Disco rigido; Unità di Backup
Accesso tramite password con frequenza di aggiornamento trimestrale
Antivirus installato con frequenza di aggiornamento giornaliera

Luogo di custodia dei backup:
Stanza economato
Indirizzo: Via S.Paolo ex IAI - MESSINA (ME)

002 - Archivio clienti, fornitori, procedure amministrative

Finalità perseguite: Gestione della clientela; Gestione dei fornitori; Trattamento economico e giuridico del personale; Formazione professionale per il personale; Adempimento di obblighi fiscali o contabili; Programmazione delle attività; Gestione del patrimonio mobiliare e immobiliare; Gestione del contenzioso; Servizi di controllo interno (sicurezza); Servizi di controllo interno (produttività); Servizi di controllo interno (qualità dei sevizi); Servizi di controllo interno (integrità del patrimonio)
Categorie di dati trattati: Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati contabili
Categorie di soggetti interessati: Clienti; Fornitori; Dipendenti; Collaboratori; Altri soggetti

Natura dei dati trattati: PERSONALI
Modalità del trattamento: INTERNO; ELETTRONICO E CARTACEO; NON CIFRATO.

Luogo di ubicazione della banca dati:
Stanza Server
Indirizzo: Via S.Paolo ex IAI - MESSINA (ME)
Attività svolta: area CED dove sono collocati i 3 Server, protetta da chiave, installato climatizzatore in uso nel perido estivo
Tipologia di accesso: Non consentito al pubblico
Tipologia di chiusura: Con serratura
Impianto di allarme: Non installato
Impianto anticendio: Non installato
Soggetti autorizzati all'ingresso nei locali: Palana Vincenzo; Sarlo Domenico; Torre Salvatore

Strumenti elettronici utilizzati: SERVER G6
Il Server G6 è il principale contenitore di Dati, e funge da Server di Backup dei Server G4 e G3. Il piano di backup schedulato è descritto in dettaglio nell' Allegato Backup

Caratteristiche dello strumento: Collegamento a internet; Collegamento a rete locale (LAN); Disco removibile; Disco rigido; Unità di Backup
Accesso tramite password con frequenza di aggiornamento trimestrale
Antivirus installato con frequenza di aggiornamento giornaliera

Luogo di custodia dei backup:
Stanza economato
Indirizzo: Via S.Paolo ex IAI - MESSINA (ME)

<u>003 - Procedure tecniche, documenti cartografici</u>

Finalità perseguite: Trattamento economico e giuridico del personale; Formazione professionale per il personale; Programmazione delle attività; Servizi di controllo interno (sicurezza); Servizi di controllo interno (produttività); Servizi di controllo interno (qualità dei sevizi); Servizi di controllo interno (integrità del patrimonio)
Categorie di dati trattati: Nominativo, indirizzo o altri elementi di identificazione personale; Informazioni sullo stato di lavoro
Categorie di soggetti interessati: Clienti; Fornitori; Dipendenti; Collaboratori; Altri soggetti

Natura dei dati trattati: PERSONALI
Modalità del trattamento: INTERNO; ELETTRONICO E CARTACEO; NON CIFRATO.

Luogo di ubicazione della banca dati:
Stanza Server
Indirizzo: Via S.Paolo ex IAI - MESSINA (ME)
Attività svolta: area CED dove sono collocati i 3 Server, protetta da chiave, installato climatizzatore in uso nel perido estivo
Tipologia di accesso: Non consentito al pubblico
Tipologia di chiusura: Con serratura
Impianto di allarme: Non installato
Impianto anticendio: Non installato
Soggetti autorizzati all'ingresso nei locali: Palana Vincenzo; Sarlo Domenico; Torre Salvatore

Strumenti elettronici utilizzati: SERVER G6
Il Server G6 è il principale contenitore di Dati, e funge da Server di Backup dei Server G4 e G3. Il piano di backup schedulato è descritto in dettaglio nell' Allegato Backup

Caratteristiche dello strumento: Collegamento a internet; Collegamento a rete locale (LAN); Disco removibile; Disco rigido; Unità di Backup

Accesso tramite password con frequenza di aggiornamento trimestrale
Antivirus installato con frequenza di aggiornamento giornaliera

Luogo di custodia dei backup:
Stanza economato
Indirizzo: Via S.Paolo ex IAI - MESSINA (ME)

6. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' (REGOLA 19.2)

6.1 Titolare del trattamento dei dati personali

Il Titolare del trattamento dei dati personali è:

- *AUTORITA' D'AMBITO A.T.O. 3 MESSINA, con sede in Messina (ME), Via S.Paolo ex IAI,* codice fiscale 97072340835, partita IVA 97072340835

Il Titolare del trattamento si impegna ad assicurare e garantire direttamente che vengano adottate le misure di sicurezza previste dal Codice in materia di protezione dei dati personali e dal 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, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più responsabili della sicurezza dei dati che assicurino e garantiscano che vengano adottate tutte le misure di sicurezza ai sensi del Codice in materia di protezione dei dati personali e del Disciplinare tecnico in materia di misure minime di sicurezza.

In base a quanto stabilito dall'Art. 29 del Codice in materia di protezione dei dati personali il Titolare del trattamento, in relazione all'attività svolta, se lo ritiene opportuno, può individuare, nominare e incaricare per iscritto, uno o più responsabili di specifici trattamenti con il compito di individuare, nominare e incaricare per iscritto, gli incaricati del trattamento dei dati personali.

Nel caso in cui il Titolare del trattamento ritenga di non nominare alcun responsabile di specifici trattamenti, ne assumerà tutte le responsabilità e funzioni.

In base a quanto stabilito dall'Art. 29 del Codice in materia di protezione dei dati personali, il Titolare del trattamento, ove necessario, per esigenze organizzative, può designare facoltativamente uno o più soggetti responsabili del trattamento anche mediante suddivisione di compiti.

6.2 Responsabile del trattamento dei dati personali

Il responsabile del trattamento dei dati personali è:

- PALANA VINCENZO, residente in MESSINA (ME), , codice fiscale PLNVCN60H30E290Y, per le seguenti banche dati: Archivio clienti, fornitori, procedure contabili, Archivio clienti, fornitori, procedure amministrative, Procedure tecniche, documenti cartografici

Il responsabile del trattamento dei dati personali viene 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.

Egli è nominato attraverso lettera di incarico, controfirmata per accettazione, in cui vengono specificate le responsabilità che gli sono affidate e le banche dati di cui è responsabile per quanto attiene alla sicurezza ed effettua il trattamento attenendosi alle istruzioni impartite dal Titolare del trattamento.

Il responsabile del trattamento ha inoltre il compito di individuare, nominare e incaricare per iscritto, gli incaricati del trattamento dei dati personali relativamente al trattamento di cui gli è stata *assegnata la responsabilità*.

Altri specifici compiti affidati al responsabile del trattamento sono:

- controllare che il trattamento venga effettuato in conformità con le previsioni del Codice in *materia di protezione dei dati personali* e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D. Lgs. n.196 del 30 giugno 2003);
- fornire adeguate istruzioni agli incaricati del *trattamento effettuato con strumenti elettronici*;
- fornire adeguate istruzioni agli incaricati del trattamento effettuato senza l'ausilio di strumenti elettronici;
- *accertare periodicamente*, e comunque almeno annualmente, che vi siano le condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento dei dati personali.

La nomina del responsabile è a tempo indeterminato e decade per revoca o dimissioni dello stesso. La nomina può essere revocata in qualsiasi momento dal titolare, senza preavviso, ed eventualmente affidata ad altro soggetto.

Ai sensi delle previsioni di cui all'articolo 30 del Codice *in materia* di protezione dei dati personali, 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 di* uno specifico trattamento di dati personali, attenendosi alle istruzioni impartite.

6.3 Responsabile della gestione e della manutenzione degli strumenti elettronici

Gli amministratori di sistema, responsabili della gestione e della manutenzione degli strumenti elettronici sono:

- PALANA VINCENZO, residente in MESSINA (ME), , codice fiscale PLNVCN60H30E290Y, per i seguenti strumenti: SERVER G6, SERVER G4, SERVER G3, SERVER PROXY, SERVER FAX

Il titolare deve informare ciascun responsabile 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 e dal Disciplinare tecnico in materia di misure minime di sicurezza.

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

Il responsabile della gestione e della manutenzione *degli strumenti elettronici ha il compito di*:

- 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;
- gestire e curare *la manutenzione della rete aziendale, della posta elettronica*, sistemi di comunicazione interna ed esterna tramite e-mail;
- definire, in conformità con le previsioni di cui al punto 16 del Disciplinare tecnico in materia di misure minime di sicurezza, l'attivazione di idonei strumenti per la protezione contro il rischio di intrusione e contro l'azione di programmi informatici volti a provocare 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. Ogni sei mesi si dovrà procedere all'aggiornamento di *tali strumenti*;
- aggiornare periodicamente, ai sensi delle previsioni di cui al punto 17 del Disciplinare tecnico in materia di misure minime di sicurezza e comunque almeno una volta l'anno, i programmi per

elaboratore utilizzati per garantire l'invulnerabilità degli strumenti elettronici e correggerne i difetti. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento deve essere almeno semestrale;
- garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso da parte di chiunque abusivamente si introduca nel sistema informatico o telematico, ai sensi delle previsioni di cui al punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza, utilizzando idonei strumenti elettronici;
- informare il Titolare del trattamento dei dati personali qualora vengano rilevati rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Nel caso in cui il titolare ritenga di non nominare alcun responsabile alla gestione e alla manutenzione degli strumenti elettronici, ne assumerà tutte le responsabilità e funzioni.

La nomina del responsabile della gestione e della manutenzione degli strumenti elettronici è a tempo indeterminato, e decade per revoca o dimissioni dello stesso; può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati personali senza preavviso, ed eventualmente affidata ad altro soggetto.

Ai sensi delle previsioni di cui punto 10 del Disciplinare tecnico in materia di misure minime di sicurezza, se l'accesso ai dati ed agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, debbono essere impartite idonee e preventive disposizioni scritte volte ad 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, in relazione all'attività svolta, se lo ritiene opportuno, individuare, nominare e incaricare per iscritto, uno o più responsabili della custodia delle copie delle credenziali.

6.4 Responsabile della custodia delle copie delle credenziali

I responsabili della custodia delle copie delle credenziali sono:

- CENTRO INFORMATICA MERIDIONALE, con sede in Messina (ME), Viale Europa 34, codice fiscale 01293580831, partita IVA 01293580831, per i seguenti strumenti: SERVER G6, SERVER G4, SERVER G3, SERVER PROXY, SERVER FAX

Il Titolare del trattamento deve informare il responsabile della custodia delle copie delle credenziali, della responsabilità che gli viene affidata in conformità a quanto stabilito dal Codice in materia di protezione dei dati personali e dal Disciplinare tecnico in materia di misure minime di sicurezza. Deve, inoltre, consegnare a ciascun responsabile 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.

Il responsabile della custodia delle copie e delle credenziali ha il compito di:

- 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;
- custodire adeguatamente le copie delle credenziali di autenticazione;
- fornire agli incaricati del trattamento idonee istruzioni sull'uso delle componenti riservate 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;
- assicurare che il Codice per l'identificazione, laddove sia stato già utilizzato, non sia assegnato ad altri incaricati del trattamento, neppure in tempi diversi;
- revocare le Credenziali di autenticazione per l'accesso ai dati degli incaricati del trattamento nel caso di mancato utilizzo per oltre 6 (sei) mesi;
- 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;
- impartire idonee istruzioni agli incaricati del trattamento per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

In caso di prolungata assenza o di impedimento di un incaricato del trattamento, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il responsabile 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:

- avvalendosi dei diritti di "amministratore di sistema", può procedere alla modifica forzosa della componente riservata delle credenziali di autenticazione dell'incaricato del trattamento dei dati personali che sia assente o impedito ad effettuare il trattamento;
- comunica la componente riservata delle credenziali di autenticazione così modificata ad un altro incaricato del trattamento designato dal responsabile del trattamento il quale potrà utilizzarla solo in via temporanea;
- 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, l'incaricato dovrà essere informato dell'intervenuta modifica e dovrà cambiare la propria componente riservata delle credenziali di autenticazione.

La nomina di uno o più responsabili della custodia delle copie delle credenziali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso; può essere revocata in qualsiasi momento dal titolare del trattamento dei dati personali senza preavviso, ed essere affidata ad altro soggetto.

Qualora il titolare del trattamento dei dati personali ritenga di non nominare alcun responsabile della custodia delle copie delle credenziali, egli ne assumerà tutte le responsabilità e funzioni.

In base alle previsioni di cui al punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza il Titolare del trattamento, in relazione all'attività svolta, se lo ritiene opportuno, può individuare, nominare e incaricare per iscritto, uno o più responsabili delle copie di sicurezza delle banche dati.

6.5 Responsabile delle copie di backup

Il responsabile delle copie di backup è:

- PALANA VINCENZO, residente in MESSINA (ME), , codice fiscale PLNVCN60H30E290Y, per le seguenti banche dati: Archivio clienti, fornitori, procedure contabili, Archivio clienti, fornitori, procedure amministrative, Procedure tecniche, documenti cartografici

Il Titolare del trattamento dei dati personali consegna a ciascun responsabile 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.

Il responsabile 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 dati personali gestite.

Al fine di assicurare l'integrità dei dati contro i rischi di distruzione o perdita, il Titolare del trattamento dei dati personali stabilisce, con il supporto tecnico del responsabile della gestione e della manutenzione degli strumenti elettronici, la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche dati trattate.

I criteri debbono essere concordati con il responsabile della gestione e della manutenzione degli strumenti elettronici in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In base alle previsioni di cui al punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza, le copie di sicurezza dei dati devono essere effettuate al massimo con frequenza settimanale.

Per ogni banca dati debbono essere definite le seguenti specifiche:

- il *tipo di supporto* che deve essere utilizzato per effettuare le copie di backup;
- il numero di copie di backup che vengono effettuate ogni volta;
- se i supporti utilizzati per le copie di backup vengono riutilizzati e in questo caso con quale periodicità;
- se per effettuare le copie di backup si utilizzano procedure automatizzate e programmate;
- le modalità di controllo delle copie di backup;
- il responsabile ha il compito di effettuare le copie di backup;
- le istruzioni e i comandi necessari per effettuare le copie di backup.

I responsabili delle copie di sicurezza delle banche dati hanno il compito di:

- adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al salvataggio periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal titolare del trattamento dei dati personali;
- verificare la qualità delle copie di sicurezza dei dati e che esse vengano conservate in luogo adatto, sicuro e ad accesso controllato;
- conservare con la massima cura e custodia i dispositivi che vengono utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale privo di autorizzazione;
- comunicare tempestivamente al responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema che si verifichi nella normale attività di copia delle banche dati.

Qualora il Titolare del trattamento dei dati personali ritenga di non nominare alcun responsabile delle copie di sicurezza delle banche dati, ne assumerà tutte le responsabilità e funzioni.

In conformità a quanto disposto dal punto 19.4 del Disciplinare tecnico in materia di misure minime di sicurezza, il Titolare del trattamento dei dati personali se lo ritiene opportuno, può individuare, nominare e incaricare per iscritto, uno o più responsabili dell'accesso ai locali in cui sono effettuati i trattamenti di dati personali o in cui vengono conservati documenti contenenti dati personali.

6.6 Incaricati del trattamento

Per il trattamento di dati personali effettuato con l'ausilio di strumenti elettronici, l'incaricato del trattamento deve osservare le seguenti disposizioni:

- può trattare esclusivamente i dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con conseguente possibilità di accedere ed

utilizzare la documentazione cartacea e gli strumenti informatici, elettronici e telematici e le 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 deve verificare che i dati trattati siano esatti e, se sono inesatti o incompleti, deve aggiornarli tempestivamente;
- ogni Incaricato del trattamento dei dati personali deve 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 dichiarate della raccolta;
- l'incaricato del trattamento dei dati personali che abbia ricevuto le credenziali di autenticazione per il trattamento dei dati personali, deve conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in suo 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 che siano 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;
- l'incaricato del trattamento non deve in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici l'incaricato del trattamento dei dati personali deve osservare le seguenti disposizioni:

- essi non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al minimo indispensabile per effettuare le operazioni di trattamento e, in ogni caso, l'incaricato del trattamento non dovrà lasciarli mai incustoditi;
- deve accertare che, se composti da numerose pagine o più raccoglitori, siano sempre completi ed integri;
- al termine dell'orario di lavoro deve riportarli nei locali individuati per la loro conservazione;
- essi non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro;
- deve essere adottata ogni cautela necessaria ad evitare che persone non autorizzate possano venire a conoscenza del loro contenuto;
- per evitare il rischio di loro diffusione, si deve limitare l'utilizzo di copie fotostatiche;
- particolare cautela deve essere adottata quando essi vengano consegnati in originale ad un altro incaricato debitamente autorizzato;
- è proibito utilizzarne copie fotostatiche (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né possono essere utilizzate come carta per appunti;
- nel caso in cui essi debbano essere portati al di fuori dei locali individuati per la loro conservazione o all'esterno del luogo di lavoro, l'incaricato del trattamento non deve mai lasciare incustodita la cartella o la borsa nella quale sono contenuti;
- è 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;
- è preferibile 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, anche accidentalmente, da soggetti non autorizzati. Queste cautele assumono particolare rilievo quando il telefono viene utilizzato in luogo pubblico o aperto al pubblico.

utilizzare la documentazione cartacea e gli strumenti informatici, elettronici e telematici e le 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 deve verificare che i dati trattati siano esatti e, se sono inesatti o incompleti, deve aggiornarli tempestivamente;
- ogni incaricato del trattamento dei dati personali deve 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 dichiarate della raccolta;
- l'incaricato del trattamento dei dati personali che abbia ricevuto le credenziali di autenticazione per il trattamento dei dati personali, deve conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in suo 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 che siano 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;
- l'incaricato del trattamento non deve in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per documenti contenenti dati personali trattati <u>senza l'ausilio di strumenti elettronici</u> l'incaricato del trattamento dei dati personali deve osservare le seguenti disposizioni:

- essi non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al minimo indispensabile per effettuare le operazioni di trattamento e, in ogni caso, l'incaricato del trattamento non dovrà lasciarli mai incustoditi;
- deve accertare che, se composti da numerose pagine o più raccoglitori, siano sempre completi ed integri;
- al termine dell'orario di lavoro deve riportarli nei locali individuati per la loro conservazione;
- essi non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro;
- deve essere adottata ogni cautela necessaria ad evitare che persone non autorizzate possano venire a conoscenza del loro contenuto;
- per evitare il rischio di loro diffusione, si deve limitare l'utilizzo di copie fotostatiche;
- particolare cautela deve essere adottata quando essi vengano consegnati in originale ad un altro incaricato debitamente autorizzato;
- è proibito utilizzarne copie fotostatiche (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né possono essere utilizzate come carta per appunti;
- nel caso in cui essi debbano essere portati al di fuori dei locali individuati per la loro conservazione o all'esterno del luogo di lavoro, l'incaricato del trattamento non deve mai lasciare incustodita la cartella o la borsa nella quale sono contenuti;
- è 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;
- è preferibile 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, anche accidentalmente, da soggetti non autorizzati. Queste cautele assumono particolare rilievo quando il telefono viene utilizzato in luogo pubblico o aperto al pubblico.

Il Titolare del trattamento consegnerà a ciascun incaricato una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

L'incaricato deve ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni affidategli e sugli adempimenti cui è tenuto.

All'incaricato del trattamento dei dati personali viene assegnata una credenziale di autenticazione. Egli deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale di autenticazione e deve custodire diligentemente i dispositivi in suo possesso ed uso esclusivo.

La nomina dell'incaricato del trattamento dei dati personali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso; può essere revocata in qualsiasi momento dal responsabile che gli ha affidato l'incarico, senza preavviso, ed eventualmente può essere affidata ad altro soggetto.

Elenco banche dati, incaricati al trattamento e relativi diritti di accesso:

Archivio clienti, fornitori, procedure contabili

- Santalco Giuseppe	LMIC
- Trovato Santi	LMIC
- Minissale Pietro	LMIC
- Cutroneo Antonio	LMIC

Archivio clienti, fornitori, procedure amministrative

- Santalco Giuseppe	LMIC
- Di Pietro Rosario	LMIC
- Palana Vincenzo	LMIC
- Trovato Santi	LMIC
- Torre Salvatore	LMIC
- Sarlo Domenico	LMIC
- Minissale Pietro	LMIC
- Cutroneo Antonio	LMIC

Procedure tecniche, documenti cartografici

- Santalco Giuseppe	LMIC
- Scarcella Santino	LMIC
- Di Pietro Rosario	LMIC
- Trovato Santi	LMIC
- Torre Salvatore	LMIC
- Sarlo Domenico	LMIC

Legenda: L=Lettura M=Modifica I=Inserimento C=Cancellazione

6. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (REGOLA 19.3)

Analisi dei rischi relativi all'accesso ai locali

1) Ingressi non autorizzati a locali/aree ad accesso ristretto

Descrizione del rischio: Possibilità di accesso ai locali da parte di persone non autorizzate.

Probabilità del rischio: Poco probabile
Entità del rischio: Medio
Valutazione globale del rischio: Medio

2) Sottrazione di strumenti contenenti dati

Descrizione del rischio: Possibilità di eventuali furti dai locali di uno o più strumenti contenenti i dati oggetto del trattamento.

Probabilità del rischio: Poco probabile
Entità del rischio: Grave
Valutazione globale del rischio: Medio

3) Guasto all'impianto elettrico

Descrizione del rischio: Possibilità di guasto all'impianto elettrico che causi gravi danni e/o cortocircuiti alle attrezzature elettroniche contenenti i dati oggetto di trattamento.

Probabilità del rischio: Poco probabile
Entità del rischio: Grave
Valutazione globale del rischio: Medio

4) Interruzione dell'energia elettrica

Descrizione del rischio: Possibilità di interruzione dell'erogazione di energia elettrica.

Probabilità del rischio: Molto probabile
Entità del rischio: Medio
Valutazione globale del rischio: Medio

5) Allagamento dei locali

Descrizione del rischio: Possibilità di allagamento dei locali.

Probabilità del rischio: Improbabile
Entità del rischio: Molto grave
Valutazione globale del rischio: Medio

6) Incendio nei locali

Descrizione del rischio: Possibilità dei incendio nei locali.

Probabilità del rischio: Improbabile
Entità del rischio: Molto grave
Valutazione globale del rischio: Medio

Analisi dei rischi relativi ai soggetti

1) Uso non autorizzato (e possibile manomissione) della strumentazione

Descrizione del rischio: Possibilità di utilizzo degli strumenti da parte di persone non autorizzate.

Probabilità del rischio: Poco probabile
Entità del rischio: Grave
Valutazione globale del rischio: Medio

2) Carenza di consapevolezza, disattenzione o incuria

Descrizione del rischio: Possibilità di causare guasti alla strumentazione hardware o software dovuti a mancata di formazione, scarsa attenzione o incuria da parte del personale.

Probabilità del rischio: Probabile
Entità del rischio: Medio
Valutazione globale del rischio: Medio

Analisi dei rischi relativi alla strumentazione software

1) Malfunzionamenti dovuti ad errori nel software (bugs)

Descrizione del rischio: Possibilità di errori nel software utilizzato per l'imputazione e la consultazione dei dati che compromettano l'integrità di questi ultimi.

Probabilità del rischio: Poco probabile
Entità del rischio: Medio
Valutazione globale del rischio: Medio

2) Infezione da virus informatici

Descrizione del rischio: Possibilità di infezione da virus informatici.

Probabilità del rischio: Probabile
Entità del rischio: Grave
Valutazione globale del rischio: Alto

3) Infezione da spyware

Descrizione del rischio: Possibilità di infezione da spyware.

Probabilità del rischio: Probabile
Entità del rischio: Grave
Valutazione globale del rischio: Alto

Analisi dei rischi relativi alla strumentazione hardware

1) Guasto

Descrizione del rischio: Possibilità di eventuali guasti alla strumentazione elettronica utilizzata per il trattamento dei dati.

Probabilità del rischio: Poco probabile
Entità del rischio: Grave
Valutazione globale del rischio: Medio

2) Degrado supporti di backup

Descrizione del rischio: Possibilità che le copie di backup della banca dati non siano più riutilizzabili a causa di degrado dei supporti di memorizzazione utilizzati.

Probabilità del rischio: Poco probabile
Entità del rischio: Grave
Valutazione globale del rischio: Medio

7. MISURE IN ESSERE DA ADOTTARE (REGOLA 19.4)

Misure preventive e correttive - rischi relativi all'accesso ai locali

1) Ingressi non autorizzati a locali/aree ad accesso ristretto

Al fine di prevenire l'ingresso da parte di persone non autorizzate ai locali in cui sono custoditi i dati personali e le copie di backup degli stessi, l'accesso è protetto a livello di stabile da portone blindato con serratura, la stanza server è protetta da chiusura.
Le finestre sono ad oltre 3 metri di altezza dal piano terra.

Esiste un sistema di sorveglianza mediate telecamera al momento non in uso che verrà attivato nel primo trimestre (salvo problematiche tecniche)

2) Sottrazione di strumenti contenenti dati

In aggiunta alle misure già previste per la prevenzione del rischio di accesso ai locali da parte di persone non autorizzate, ed in particolare per la protezione durante le ore notturne ed i giorni non lavorativi, il locale è controllato da un custode che risiede accanto ai locali.

3) Guasto all'impianto elettrico

L'impianto elettrico è certificato ai sensi della Legge n. 46 del 5 marzo 1990.

Inoltre le apparecchiature elettroniche contenenti i dati oggetto del trattamento sono collegate alla rete elettrica tramite apposite prese antifulmine e protette contro gli sbalzi di tensione.

4) Interruzione dell'energia elettrica

Per evitare danneggiamenti alle apparecchiature elettroniche contenenti i dati oggetto del trattamento causate da una improvvisa interruzione dell'erogazione di energia elettrica, esse sono collegate a gruppi di alimentazione elettrogeni (UPS).

5) Allagamento dei locali

Per evitare il più possibile eventuali danneggiamenti alle apparecchiature elettroniche contenenti i dati oggetto del trattamento a causa di eventuale allagamento dei locali, esse sono poste in posizione rialzata da terra.

6) Incendio nei locali

I locali sono dotati di appositi estintori da utilizzarsi per l'estinzione delle fiamme in caso di incendio. Una copie di backup è conservate in apposito armadio (a pareti ignifughe).

Misure preventive e correttive - rischi relativi ai soggetti

1) Uso non autorizzato (e possibile manomissione) della strumentazione

L'accesso allo strumento è subordinato alla digitazione di un "nome utente" accoppiato ad una "password".

In caso di interruzione temporanea dell'attività lavorativa è obbligatorio utilizzare uno "screen saver" che, al momento della ripresa dell'attività stessa, richieda nuovamente la password di accesso.

L'aggiornamento della password è effettuato periodicamente secondo quanto previsto nell'apposita sezione del D.P.S.

2) Carenza di consapevolezza, disattenzione o incuria

Gli utilizzatori sono già edotti sul corretto utilizzo degli strumenti ed è previsto un piano formativo periodico per un corretto e migliore utilizzo.

Sono inoltre previsti periodici corsi di formazione ed aggiornamento professionale, come specificato nell'apposita sezione del D.P.S.

Al fine di evitare possibili perdite di dati dovute a cancellazioni erronee si è previsto un piano di backup giornaliero dei dati.

Misure preventive e correttive - rischi relativi alla strumentazione software

1) Malfunzionamenti dovuti ad errori nel software (bugs)

Per ridurre al minimo le possibilità di bugs, per ciascun software utilizzato viene verificata la presenza di un aggiornamento (o service pack) direttamente dal sito del produttore. Ove richiesto, sono stati stipulati appositi contratti di aggiornamento.

Al fine di evitare possibili perdite di dati dovute a errori nel software di trattamento, si è previsto un piano di backup giornaliero dei dati.

2) Infezione da virus informatici

Per evitare i danni derivanti dalla presenza di virus informatici sui sistemi utilizzati per il trattamento dei dati personali, vengono utilizzati appositi software antivirus aggiornati quotidianamente. Tutti i Pc e Server navigano su Internet protetti da un Firewall e gestiti da Proxy Server, ambedue aggiornati automaticamente.

I programmi antivirus utilizzati devono avere sempre l'opzione di "auto-protezione" attivata.

Settimanalmente ogni PC deve essere sottoposto ad una scansione antivirus.

Al fine di evitare possibili perdite di dati dovute a infezioni da virus informatici, si è previsto un piano di backup giornaliero dei dati.

3) Infezione da spyware

Per evitare l'intercettazione di informazioni in rete (attraverso una infezione da "spyware"), oltre alle misure adottate per la protezione dai virus, è previsto - ove possibile - l'installazione di un programma firewall.

I sistemi Windows XP e Windows 7 vengono aggiornati all'ultimo service pack, che garantisce una maggiore protezione attraverso un firewall integrato.

Periodicamente ogni PC utilizzato dovrà essere sottoposto alla scansione con programmi di tipo "anti-spyware".

Misure preventive e correttive - rischi relativi alla strumentazione hardware

1) Guasto

Per prevenire possibili guasti si procede periodicamente ad un controllo di funzionalità con eventuale sostituzione dei componenti danneggiati.

Al fine di evitare possibili perdite di dati dovute a guasti alla strumentazione elettronica utilizzata per il trattamento si è previsto un piano di backup giornaliero dei dati. Tutti i computer con funzionalità rilevanti sono protetti da UPS.

2) Degrado supporti di backup

Per evitare il degrado dei supporti si prevede una sostituzione periodica degli stessi (in particolare nel caso di supporti riscrivibili).

I supporti di backup vengono conservati in posizioni fisicamente distinte e separate dai sistemi in uso, per evitare che in caso di furto, incendio, alluvione o altro evento catastrofico, le copie non siano più disponibili o utilizzabili.

8. CRITERI E MODALITÀ DI RIPRISTINO DEI DATI (REGOLA 19.5)

Ai sensi delle previsioni di cui al punto 23 del Disciplinare tecnico in materia di misure minime di sicurezza, il Titolare del trattamento deve adottare idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e comunque non superiori a sette giorni.

Una volta valutata l'assoluta necessità di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento, il Titolare del trattamento deve provvedere all'operazione di ripristino dei dati con la collaborazione del responsabile dei backup e del responsabile della manutenzione degli strumenti elettronici.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti, è compito esclusivo del Titolare del trattamento che si può avvalere del parere del responsabile della manutenzione degli strumenti elettronici.

Le copie di sicurezza vengono effettuate come segue:

- Archivio clienti, fornitori, procedure contabili con frequenza di backup giornaliera
- Archivio clienti, fornitori, procedure amministrative con frequenza di backup giornaliera
- Procedure tecniche, documenti cartografici con frequenza di backup giornaliera

Al fine di garantire l'effettiva possibilità di ripristino, le copie vengono custodite in locali distaccati da quelli in cui sono situati i vari supporti di memorizzazione, chiusi a chiave e la cui custodia è affidata al responsabile dell'accesso ai locali.

Ogni tre mesi si dovrà effettuare un test di recupero dei dati dalla copia, al fine di verificare l'efficienza del sistema.

9. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI (REGOLA 19.6)

Il responsabile del trattamento valuta per ogni incaricato a cui è stato affidato il trattamento stesso, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, la necessità di pianificare eventuali interventi formativi.

La formazione è programmata già al momento dell'ingresso in servizio di nuovi incaricati nonché quando intervengano cambiamenti di mansioni oppure vengano introdotti nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Il Titolare del trattamento dei dati personali, in collaborazione con il responsabile del trattamento, deve redigere ogni anno, entro il 31 marzo, il piano di formazione del personale specificando le necessità di ulteriore formazione del personale stesso.

Il Piano di formazione del personale deve essere predisposto per:

- informare gli incaricati del trattamento sui rischi che incombono sui dati nonché sulle misure disponibili per prevenire eventi dannosi;
- informare gli incaricati del trattamento sui profili della disciplina della protezione dei dati personali più rilevanti in rapporto alle relative attività;
- informare gli incaricati del trattamento sulle responsabilità che ne derivano;
- informare gli incaricati del trattamento sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Tutti gli incaricati del trattamento dovranno prendere visione del DPS e nelle singole lettere di conferimento degli incarichi dovranno essere indicati tutti i rischi che incombono sulla sicurezza dei dati, nonché le misure necessarie previste. Il responsabile del trattamento è anche responsabile della formazione di ogni suo incaricato.

Ogni incaricato del trattamento dovrà dichiarare di essere a conoscenza delle misure di sicurezza messe in atto e garantirne il pieno rispetto; dovrà, inoltre, garantire di dare corretta attuazione alle previsioni del Codice in materia di protezione dei dati personali.

Qui di seguito si elencano i corsi di formazione aziendali già effettuati, in corso di svolgimento o pianificati per il futuro:

1) Istruzione e modalità di backup dati

Data di inizio prevista: 14/01/2013 Ore totali previste: 1
Data di inizio effettiva: Data di conclusione:

Descrizione completa: Le date sono soggette a variazioni

Finalità: La formazione è mirata a monitorare il corretto funzionamento delle procedure automatizzate di backup, capirne la logica, sapere cosa fare in caso di perdita di dati, guasti, ecc. che comportino il ripristino di singolo file o di interi volumi.

Elenco dei partecipanti:
- Santalco Giuseppe
- Scarcella Santino
- Di Pietro Rosario
- Palana Vincenzo
- Trovato Santi
- Torre Salvatore
- Sarlo Domenico
- Centro Informatica Meridionale

- *Collaboratori Esterni (autorizzati)*
- Minissale Pietro
- Cutroneo Antonio

2) Istruzione sulle modalità di accesso in sicurezza

Data di inizio prevista: 14/01/2013 Ore totali previste: 1
Data di inizio effettiva: Data di conclusione:

Descrizione completa: Le date sono soggette a variazioni

Finalità: La formazione è finalizzata a formare gli operatori per un corretto accesso ai Server in sicurezza, a proteggere le proprie credenziali, ad informare su come comportarsi in caso di smarrimento delle credenziali od in caso di furto delle stesse, presa di coscenza delle responsabilità.

Elenco dei partecipanti:
- Santalco Giuseppe
- *Scarcella Santino*
- Di Pietro Rosario
- Palana Vincenzo
- Trovato Santi
- Torre Salvatore
- Sarlo Domenico
- Centro Informatica Meridionale
- Collaboratori Esterni (autorizzati)
- Minissale Pietro
- *Cutroneo Antonio*

3) Istruzione su utilizzo in sicurezza del proprio Pc

Data di inizio prevista: 14/01/2013 Ore totali previste: 1
Data di inizio effettiva: Data di conclusione:

Descrizione completa: Le date sono soggette a variazioni

Finalità: Il corso è mirato a dare una formazione per la navigazione su Internet in sicurezza e rendere gli operatori edotti sui rischi di una navigazione su siti (a rischio); Siti permessi e non; Download autorizzati e non; divieto di installazione di software non autorizzati; controllare lo stato del proprio antivirus; controllo delle periferiche di massa USB, HD, ecc. prima del loro utilizzo; Pop-up Internet; cosa fare in caso di sospetto Virus o violazione del sistema; segnalazioni all'amministratore di sistema; informazione sulla registrazione e monitoraggio su Log e registro di accesso delle pagine Internet visitate; non autorizzazione alla navigazione privata su siti non permessi; messa a disposizione di stazione dedicata per eventuali utilizzi personali e non lavorativi.

Elenco dei partecipanti:
- Santalco Giuseppe
- Scarcella Santino
- Di Pietro Rosario
- Palana Vincenzo
- Trovato Santi
- Torre Salvatore
- Sarlo Domenico
- *Centro Informatica Meridionale*
- Collaboratori Esterni (autorizzati)

- Minissale Pietro
- Cutroneo Antonio

4) Istruzione sul corretto posizionamento dei Files

Data di inizio prevista: 14/01/2013 Ore totali previste: 2
Data di inizio effettiva: Data di conclusione:

Descrizione completa: Le date sono soggette a variazioni

Finalità: La formazione è finalizzata ad indicare la corretta nomenclatura dei files ed il loro posizionamento sulle aree condivise o personali, acquisire gli standard prefissati dal responsabile della rete. Informare che il backup dei dati è centralizzato e non riguarda il fisico Pc di ogni operatore e che in caso di guasto tutti i dati verrano persi con responsabilità dello stesso operatore / utilizzatore.

Elenco dei partecipanti:
- Santalco Giuseppe
- Scarcella Santino
- Di Pietro Rosario
- Palana Vincenzo
- Trovato Santi
- Torre Salvatore
- Sarlo Domenico
- Centro Informatica Meridionale
- Collaboratori Esterni (autorizzati)
- Minissale Pietro
- Cutroneo Antonio

10. TRATTAMENTI AFFIDATI ALL'ESTERNO (REGOLA 19.7)

Il Titolare del trattamento dei dati personali può decidere di affidare il trattamento stesso a soggetti esterni alla struttura; in questo caso deve redigere ed aggiornare ad ogni variazione l'elenco degli stessi, indicando:

- i soggetti interessati
- i luoghi dove fisicamente avviene il trattamento dei dati stessi
- i responsabili del trattamento dei dati personali

Se, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del Titolare, vi sia la possibilità di nominare quali responsabili del trattamento, soggetti controllabili dal Titolare del trattamento stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso), è possibile indicare gli stessi quali Responsabili del trattamento in Out-sourcing.

Qualora ciò non sia possibile, si potranno indicare, in quanto soggetti autonomi, i Titolari autonomi del trattamento in Out-sourcing, per il quale trattamento, ai sensi dell'art. 28 del Codice in materia di protezione dei dati personali, devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

Criteri per la scelta degli enti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare

Il Titolare a cui è stato affidato il trattamento dei dati all'esterno deve rilasciare una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento.

Nomina del responsabile del trattamento in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura, il Titolare del trattamento dei dati personali deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

La nomina del responsabile del trattamento in Out-sourcing viene effettuata con lettera che deve essere controfirmata per accettazione. Copia di essa è conservata a cura del Titolare del trattamento dei dati personali in luogo sicuro.

Il Titolare del trattamento dei dati personali deve informare il responsabile del trattamento in Out-sourcing, dei compiti che gli sono assegnati in conformità a quanto disposto dal Codice in materia di protezione dei dati personali e dal Disciplinare tecnico in materia di misure minime di sicurezza.

Al momento dell'affidamento dell'incarico il responsabile del trattamento in Out-sourcing, deve dichiarare per iscritto di:

- essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e sono pertanto soggetti alle previsioni del codice per la protezione dei dati personali;
- ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
- adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
- impegnarsi a rendere una relazione annuale sulle misure di sicurezza adottate e informare tempestivamente il proprio committente in caso di situazioni anomale o di emergenze;
- riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Nomina del titolare autonomo del trattamento in Out-sourcing

Per *ogni trattamento affidato* ad un soggetto esterno alla struttura, il Titolare del trattamento dei dati personali deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per *il trattamento interno*.

La nomina del titolare autonomo del trattamento *in Out-sourcing viene effettuata con lettera che* deve essere controfirmata per accettazione. Copia di essa è conservata a cura del Titolare del trattamento dei dati personali in luogo sicuro.

Il Titolare del trattamento dei dati personali deve informare il responsabile del trattamento in Out-sourcing, dei compiti che gli sono assegnati in conformità a quanto disposto dal Codice in materia di protezione dei dati personali e dal Disciplinare tecnico in materia di misure minime di sicurezza.

Al momento dell'affidamento dell'incarico il titolare autonomo del trattamento in Out-sourcing, deve *dichiarare per iscritto di:*

- essere consapevole *che i dati che tratterà nell'espletamento dell'incarico* ricevuto, sono dati personali e sono pertanto soggetti alle previsioni del codice per la protezione dei dati personali;
- ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
- adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
- impegnarsi a rendere una relazione annuale sulle misure di sicurezza adottate e informare tempestivamente il proprio committente in caso di situazioni anomale o di emergenze;
- *riconoscere il diritto* del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

In ogni caso di affidamento del trattamento dei dati personali all'esterno, la trasmissione dei dati stessi dovrà avvenire *in busta chiusa riservata all'incaricato esterno, oppure, se* i dati vengono trasmessi in forma digitale, adottando tutte le cautele necessarie a garantirne l'integrità e la riservatezza.

11. CIFRATURA DEI DATI, SEPARAZIONE DEI DATI IDENTIFICATIVI (REGOLA 19.8)

Dalle analisi effettuate non emerge la presenza di dati idonei a rivelare lo stato di salute e/o la vita sessuale degli individui. Non sussiste, pertanto, l'obbligo di ottemperare alle disposizioni di cui all'articolo 22, comma 6 del Codice in materia di protezione dei dati personali.