

Tutela dei dati personali in SERVIZI SOCIOSANITARI VAL SERIANA S.r.l.

Messa a Norma

DOCUMENTO

PROGRAMMATICO

sulla SICUREZZA

dei DATI PERSONALI

REVISIONE 2011

STUDIO LEGALE IMPERIALI

© **STUDIOLEGALEIMPERIALI**

Via Santa Croce, 4 • 20122 Milano

Tel. +39.02.8392.566 • Fax +39.02.8941.3028

Via Depretis 31 • 80133 Napoli

Tel. +39.081.4202.011 • Fax +39.081.4202.036

www.studioimperiali.com

indice

1. INTRODUZIONE	4
1.1 SCOPO DEL DOCUMENTO	4
1.2 CONTENUTI	4
1.3 PRINCIPI GENERALI.....	4
1.4 DEFINIZIONI	5
2. ELENCO DEI TRATTAMENTI	8
3. COMPITI E RESPONSABILITA'	10
3.1 TITOLARE DEI TRATTAMENTI	10
3.2 RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI.....	10
3.3 TRATTAMENTI INFORMATICI	10
3.4 RESPONSABILE DEI TRATTAMENTI INFORMATICI (RESPONSABILE DEI SISTEMI INFORMATIVI).	11
3.5 INCARICATI DEL TRATTAMENTO.....	11
3.6 AMMINISTRATORI DEI SISTEMI INFORMATICI	11
4. ANALISI DEI RISCHI	11
4.1 AREE DI ANALISI.....	ERRORE. IL SEGNALIBRO NON È DEFINITO.
4.2 INDICI DI RISCHIO.....	ERRORE. IL SEGNALIBRO NON È DEFINITO.
4.3 SINTESI	ERRORE. IL SEGNALIBRO NON È DEFINITO.
5. MISURE DI SICUREZZA	16
5.1 MISURE PER LA SICUREZZA FISICA.	16
5.2 MISURE PER LA SICUREZZA LOGICA.....	17
5.3 MISURE PER LA SICUREZZA DELLE COMUNICAZIONI.	19
6. CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI.....	20

indice p/2

7. INTERVENTI FORMATIVI	21
8. TRATTAMENTI AFFIDATI ALL' ESTERNO	22
9. NORME PER GLI INCARICATI DEL TRATTAMENTO	23
9.1 NORME DI CARATTERE GENERALE	23
9.2 COMPILAZIONE DELLE CARTELLE PSICO-SOCIALI	23
9.3 USO DELLE WORKSTATION.....	23
9.4 STAMPANTI E FAX	24
9.5 USO DELLE PASSWORD	24
9.6 INTERNET	24
10. VERIFICA DELLO STATO DELLA SICUREZZA.....	25
10.1 VERIFICHE DELL' ARCHITETTURA DI SICUREZZA	25
10.2 PROCESSO DI PREVENZIONE E ALLARME (ALERT)	25
10.3 ATTACCHI SISTEMATICI	25
10.4 INCIDENTI DI SICUREZZA.....	25
10.5 GESTIONE DEI LOG	26
11. DISPONIBILITÀ, DA PARTE DELL'AZIENDA, DEGLI STRUMENTI E DEI DATI AFFIDATI AL DIPENDENTE.....	27
12. CONTROLLI E AUDIT	28
13. REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	29

1. INTRODUZIONE

1.1 SCOPO DEL DOCUMENTO

Scopo di questo documento (di seguito "DPS") è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare presso SERVIZI SOCIO SANITARI VAL SERIANA S.r.l. (di seguito S.S. VAL SERIANA) affinché siano rispettati gli obblighi, in materia di sicurezza, previsti dal decreto legislativo 196/2003 (di seguito chiamato Codice Privacy o anche Legge), e dal Disciplinare tecnico (di seguito Disciplinare) relativo alle misure minime di sicurezza obbligatorie per il trattamento dei dati personali contenuti in qualsiasi documentazione, cartacea od in formato elettronico.

È inoltre scopo del presente documento definire le protezioni di sicurezza per le altre informazioni di cui S.S. VAL SERIANA è proprietaria e che non sono assoggettate alla suddetta Legge ma che sono critiche per l'attività di S.S. VAL SERIANA (di seguito chiamate informazioni aziendali).

Questo documento è valido per tutti quei trattamenti di cui S.S. VAL SERIANA è Titolare e per quelli di cui S.S. VAL SERIANA è nominata Responsabile da altre società, o Enti pubblici senza avere ricevuto da queste esplicite indicazioni più restrittive in materia.

1.2 CONTENUTI

In base a quanto previsto dal disciplinare tecnico (all. B del D.lgs. 196/2003) la struttura del DPS risulta composta dalle sezioni seguenti:

- elenco dei trattamenti di dati personali;
- distribuzione dei compiti e delle responsabilità;
- analisi dei rischi cui sono soggetti i dati personali;
- misure atte a garantire integrità e disponibilità dei dati, definite nelle aree della sicurezza fisica, sicurezza logica, sicurezza delle trasmissioni;
- criteri e modalità di ripristino dei trattamenti a seguito di danneggiamento o distruzione;
- piano di interventi formativi per gli incaricati del trattamento;
- criteri per garantire l'adozione delle misure minime di sicurezza per i trattamenti affidati a strutture esterne;
- criteri per la cifratura oppure la separazione dei dati relativi alla salute ed alla vita sessuale degli individui.

1.3 PRINCIPI GENERALI

Il presente DPS si applica a tutte le strutture di S.S. VAL SERIANA ed il suo contenuto deve essere divulgato a tutti anche attraverso adeguati momenti informativi e formativi.

Tutti i dipendenti di S.S. VAL SERIANA devono rispettare le prescrizioni in esso contenute ed operare, nell'ambito della propria organizzazione, in modo da:

- minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi cartacei contenenti dati personali o aziendali;
- minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali o aziendali;

- minimizzare la probabilità che i trattamenti dei dati personali o aziendali siano modificati senza autorizzazione.

NOTA: poiché dati personali sia comuni che sensibili sono presenti negli stessi ambienti e sugli stessi supporti di elaborazione, S.S. VAL SERIANA ha deciso che, in attesa di procedere ad una loro differenziazione, le misure indicate nel presente documento per i dati sensibili si applichino indifferentemente ad entrambi i tipi di informazione.

1.4 DEFINIZIONI

Dato personale

Qualunque informazione relativa a persona fisica, persona giuridica, Ente o Associazione, identificati o identificabili - anche indirettamente - mediante riferimento a qualsiasi altra informazione.

Dato pubblico

Dato proveniente da Pubblici Registri, elenchi, atti o documenti conoscibili da chiunque.

Dato particolare (sensibile e/o giudiziario)

Dato idoneo a rivelare:

- l'origine razziale ed etnica;
- le convinzioni religiose, filosofiche o di altro genere;
- l'adesione a partiti, sindacati, associazioni, organizzazioni a carattere religioso, filosofico, politico o sindacale;
- lo stato di salute e la vita sessuale;
- lo stato di indagato o di imputato in un processo penale.

Banca dati

Qualunque complesso di dati, personali o di altro tipo, organizzati secondo una pluralità di criteri per il trattamento.

Misure di sicurezza

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali volte a ridurre al minimo i rischi di distruzione o perdita - anche accidentale - dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Risorse informative

Le informazioni oggetto dei trattamenti dei dati personali sono chiamate "Risorse personali" e sono classificate in:

- Risorse o dati personali comuni.
- Risorse o dati personali sensibili.

Le risorse devono essere classificate a cura dei rispettivi proprietari.

E' responsabilità dei proprietari individuare i dati personali sensibili e i dati aziendali riservati ed informare gli Amministratori di sistema della loro collocazione.

Archivi

Gli archivi che contengono le risorse informative possono essere informatici o cartacei.

Archivi informatici

Gli archivi informatici si presentano, ad esempio, nei seguenti supporti: dischi fissi di Personal Computer (Client e Server), dischi removibili (es. Compact Disc, DVD, apparati speciali di memorizzazione), nastri magnetici, supporti ottici ed altri minori.

Archivi cartacei

Sono definiti archivi cartacei tutti i supporti, ad esclusione di quelli informatici, che contengono in qualunque forma dati o informazioni personali incluse le copie su carta, di dati gestiti con supporti informatici. Sono inclusi in questa tipologia, oltre ai dati su carta o supporto analogo le foto, le microfiches, i film, i videotape, ecc. comprese le copie, anche parziali, su supporti non informatici, di banche dati gestiti in modo automatizzato.

Archivi critici

Sono definiti archivi critici gli archivi, informatici e non, che contengono quantità significative di dati o informazioni personali sensibili o informazioni aziendali riservate.

Aree aziendali

Sono definite "Aree aziendali" tutti i locali in uso da una delle strutture costituenti S.S. VAL SERIANA, nei quali si svolgono le normali operazioni aziendali.

Ai fini della sicurezza sono considerate aree aziendali anche i locali o gli armadi eventualmente situati presso terzi (ad esempio presso fornitori, ecc.) e comunque utilizzati da personale di S.S. VAL SERIANA.

Aree ad accesso controllato

Sono definite "Aree ad Accesso Controllato" quei locali all'interno delle "Aree aziendali" che contengono *archivi critici o apparecchiature informatiche critiche*, come in seguito definite.

Risorse critiche del sistema operativo

Gli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati (es. log di sistema, tabelle di servizio, cataloghi dei dati, etc.) sono chiamate "Risorse critiche del sistema operativo".

Supporti di memorizzazione

Sono considerati *supporti di memorizzazione*, a titolo esemplificativo, i nastri magnetici, i dischi magnetici (floppy disc), i supporti speciali di memorizzazione (es. pen drive, memory card), i dischi ottici removibili e i CD-ROM che contengono informazioni personali o aziendali.

Connessioni con l'esterno

Sono considerate connessioni con l'esterno:

- interconnessioni tra il servizio IT di S.S. VAL SERIANA ed il servizio elaborazione dati di altre aziende, clienti, fornitori, outsourcer e fornitori di servizi Internet;
- accesso remoto da parte di dipendenti di S.S. VAL SERIANA o di altre aziende (fornitori, clienti, etc.).

Gateway

E' definito Gateway per le interconnessioni esterne l'insieme di hardware, software e applicazioni che permettono l'interconnessione o l'accesso remoto.

I gateway di interconnessione esterna devono essere sotto il controllo di S.S. VAL SERIANA o di sua consociata e approvati dal Responsabile dei trattamenti Informatici.

Incidenti di sicurezza

In linea generale viene definito *incidente di sicurezza* qualunque evento inaspettato che riguardi l'integrità, la riservatezza o la disponibilità delle informazioni.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

2. ELENCO DEI TRATTAMENTI

Ai fini del D.lgs 196/2003, sono stati rilevati i seguenti trattamenti, per ciascuno dei quali sono indicate le finalità, le categorie di individui interessati, le tipologie di dati coinvolti e la eventuale presenza di informazioni sensibili 1.

Finalità	Interessati	Dati	Dato Sensibile ¹
Amministrazione e Retribuzione del personale	Dipendenti	Anagrafiche	
		Dati retributivi	
		Dati professionali	
		Stato Civile e familiare	
		Curriculum	✓
		Certificati medici	✓
	Collaboratori, Stagisti	Anagrafiche	
		Dati retributivi	
		Dati professionali	
		Curriculum	✓
Amministrazione e contabilità	Utenti, Familiari degli utenti	Anagrafiche	
		Coordinate bancarie	
		Dati per intestazione fatture	
Gestione Fornitori	Cooperative, Residenze sanitarie anziani, Oratori e parrocchie, ASL, Associazioni di volontariato, Comuni e Comunità Montane	Anagrafiche	
		Dati contabili	
		Anagrafica punto di contatto	
Igiene e sicurezza del lavoro	Dipendenti e collaboratori	Anagrafiche corsisti	
		Dati professionali	
	Consulenti	Anagrafiche	
Servizi a Gestione Diretta	Minori, Familiari dei minori	Anagrafiche	
		Cartella psico-sociale	✓
		Documentazione organi giudiziari	✓
Intercultura	Minori, Familiari dei minori	Anagrafiche	
		Cartella	✓
Servizi a Gestione Indiretta	Disabili, Familiari dei disabili	Anagrafiche	
		Verbali di invalidità	✓
		Cartella psico-sociale	✓
		Stato di famiglia	
	Anziani, Familiari degli anziani	Anagrafiche	
		Stato di famiglia	
		Verbali di invalidità	✓
		Schede sanitarie e sociali	✓
		Progetto assistenziale individualizzato	✓
Debito informativo (vs ASL)	Anziani, Familiari degli anziani	Anagrafiche	
		Indice invalidità sociale/sanitario	✓

¹ La normativa in materia definisce "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 dati personali idonei a rivelare lo stato di salute e la vita sessuale. Inoltre, per gli effetti del presente documento, sono assimilati ai dati sensibili quelli idonei a rivelare la sussistenza di provvedimenti giudiziari anche se non ancora definitivi.

Questo elenco, per i trattamenti che coinvolgono dati sensibili ed eventualmente giudiziari, deve essere mantenuto aggiornato indipendentemente dalla revisione annuale del DPS. Infatti le contromisure devono essere messe in atto prima dell'inizio del trattamento, perciò l'individuazione dei nuovi trattamenti e l'applicazione delle relative protezioni devono essere condotte in parallelo. Invece l'elenco dei trattamenti che NON coinvolgono dati sensibili sarà aggiornato in occasione dell'aggiornamento annuale del DPS.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

3. COMPITI E RESPONSABILITA'

I termini Titolare, Responsabile, Incaricato del Trattamento sono usati in conformità alle definizioni del D.lgs 196/2003.

3.1 TITOLARE DEI TRATTAMENTI

Titolare dei trattamenti dei dati personali è S.S. VAL SERIANA rappresentata pro-tempore nella persona del legale rappresentante.

Al Titolare competono le decisioni in ordine alle finalità ed alle modalità di trattamento dei dati personali.

Il Titolare ha, inoltre, il compito di vigilare - anche tramite verifiche periodiche - sul rispetto, da parte dei Responsabili ed Incaricati, delle proprie istruzioni, nonché sull'osservanza delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3.2 RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI.

Il Titolare ha individuato il Dott. Marino Maffei, Direttore della Società, quale Responsabile interno dei trattamenti di dati personali, cui competono le seguenti responsabilità:

- nominare gli Incaricati al trattamento;
- promuovere lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel presente DPS;
- garantire l'attuazione delle misure di sicurezza descritte in questo documento;
- sviluppare ed attuare un programma di controllo e monitoraggio dei trattamenti e del rispetto delle norme del presente DPS;
- valutare almeno annualmente il livello ed il tipo di rischi a cui sono esposti i dati personali oggetto di trattamento;
- garantire lo svolgimento di un continuo processo di formazione degli Incaricati.

3.3 TRATTAMENTI INFORMATICI

Sono definiti trattamenti informatici tutti quei trattamenti tipici della gestione dei Sistemi Informativi e che non sono assegnabili, come responsabilità, al Responsabile.

In tale definizione sono inclusi (tale lista è fornita a solo titolo di esempio e non è da considerarsi esaustiva):

- gestione tecnica dei sistemi e dei DBM;
- gestione dei Log;
- gestione tecnica degli archivi;
- gestione delle copie di backup;
- gestione delle librerie;
- riorganizzazione delle banche dati.

Tutto il personale appartenente all' area Sistema Informativo è nominato Incaricato per questo trattamento.

3.4 RESPONSABILE DEI TRATTAMENTI INFORMATICI (RESPONSABILE DEI SISTEMI INFORMATIVI).

S.S. VAL SERIANA ha individuato il Responsabile dei trattamenti informatici il quale, oltre a quanto sopra previsto, ha anche le seguenti responsabilità aggiuntive:

- operare come custode delle applicazioni, delle banche dati, e della rete assegnate alla propria gestione;
- definire le procedure di gestione delle User-ID – normali e con autorità - e delle password;
- gestire le copie di dati e programmi, per assicurarne il ripristino dopo danni o distruzione;
- garantire l'attuazione delle misure di sicurezza descritte nel DPS e mantenere aggiornato il DPS secondo l'evoluzione tecnologica.

3.5 INCARICATI DEL TRATTAMENTO

Nell'ambito del trattamento assegnato, il personale dipendente ha ricevuto dal Responsabile la nomina ad Incaricato; è altresì Incaricato il personale non dipendente che opera per S.S. VAL SERIANA su nomina di quest' ultima oppure di un Responsabile esterno.

Gli Incaricati hanno le seguenti responsabilità:

- effettuare i trattamenti secondo le prescrizioni contenute nel presente DPS e le direttive ricevute dal Titolare e/o dal Responsabile dei trattamenti;
- rispettare le norme di sicurezza contenute nel presente DPS;
- non modificare i trattamenti esistenti e non introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile dei trattamenti;
- informare il Responsabile dei trattamenti in caso di incidente di sicurezza che coinvolga dati personali o aziendali.

3.6 AMMINISTRATORI DEI SISTEMI INFORMATICI

Con la qualifica di Amministratori dei sistemi informatici, secondo il provvedimento del Garante del 27 novembre 2008, si devono identificare coloro che sono addetti alla gestione ed alla manutenzione di un impianto di elaborazione, costituito da sistemi, reti, basi dati; ma, sempre secondo il Garante, vanno considerati anche coloro che svolgono attività tecniche quali il salvataggio di dati, organizzazione delle strutture di rete, gestione dei supporti di memorizzazione, manutenzione hardware.

In linea con queste considerazioni, i compiti degli Amministratori di sistema sono i seguenti e possono essere ritagliati sulle singole persone in rapporto alle mansioni affidate:

- sovrintendere alle risorse dei sistemi operativi degli elaboratori, delle reti, dei sistemi delle base dati e consentirne l'utilizzazione;
- sviluppare, realizzare e mantenere aggiornate, per le banche dati gestite con sistemi informatici, le misure di sicurezza in accordo con le norme contenute nel DPS;
- monitorare, se richiesto, i piani di adeguamento sulla sicurezza;
- fornire guida e supporto agli Incaricati;
- svolgere le attività tecniche specificamente assegnate, quali ottenimento delle copie di sicurezza, gestione dei supporti di memorizzazione, manutenzione di programmi e apparati, abilitazione e disabilitazione di punti di accesso alle reti;

- nell'ambito delle responsabilità assegnate e quando richiesto, effettuare periodici controlli e verifiche tecniche, anche nei riguardi dei Responsabili ed Incaricati esterni, in merito al rispetto delle prescrizioni contenute nel presente Documento;
- creare e distribuire le password agli incaricati e controllare gli strumenti meccanografici necessari per amministrare questa gestione;
- amministrare la sicurezza mantenendo aggiornati gli User-Id ed i profili di accesso ai sistemi, alle applicazioni ed alle banche dati secondo le esplicite autorizzazioni ricevute dai Responsabili;
- mantenere una traccia di audit di tutte le operazioni effettuate.

Chi possiede autorità di sistema può impropriamente operare in modo da alterare il sistema di controllo accessi, così come - ad esempio - un amministratore di sicurezza può impropriamente alterare i componenti del sistema.

Tali le posizioni vanno quindi adeguatamente responsabilizzate e formate rendendo inequivocabile quale sia l'uso improprio o illegittimo dell'autorità conferita.

Le attività che competono a tali persone devono essere esplicitamente autorizzate attraverso lettere di nomina che indichino le loro responsabilità.

Inoltre è richiesto che gli accessi effettuati con profili di amministrazione vengano registrati in appositi log inalterabili, che devono essere conservati per almeno 6 mesi.
[S.S. VAL SERIANA, allo scopo, ha pianificato la configurazione e l'attivazione dei suddetti log entro ottobre 2011]

Infine è richiesto che almeno una volta all'anno sia condotta una verifica con lo scopo di accertare che le attività svolte dagli amministratori di sistema non siano state eccedenti rispetto ai compiti loro affidati.

[S.S. VAL SERIANA, allo scopo, ha pianificato di effettuare tale verifica entro l'anno in corso]

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

4. ANALISI DEI RISCHI

L'analisi dei rischi cui sono soggetti i dati personali è focalizzata sulle circostanze, possibili o probabili, che possono determinare il verificarsi di rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta.

L'analisi dei rischi è finalizzata alla verifica del livello di sicurezza in merito ai principi di:

- **integrità dei dati** intesa come la gestione dell'accuratezza e completezza delle informazioni e delle relative applicazioni, la salvaguardia dell'esattezza dei dati, la difesa da manomissioni o modifiche non autorizzate, ecc.;
- **riservatezza, o confidenzialità dei dati** intesa come la garanzia che le informazioni siano accessibili solo alle persone autorizzate, la protezione delle trasmissioni, il controllo degli accessi, ecc.;
- **disponibilità dei dati** intesa come l'assicurazione che l'accesso ai dati sia disponibile quando necessario, quindi la garanzia per gli utenti della fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi stessi.

4.1 INDICI DI RISCHIO

Gli indici di rischio sono fissati mediante una scala a 3 valori sotto riportata.

Rischio «basso»:	<ul style="list-style-type: none">• Situazione in linea con gli standard di sicurezza più diffusi;• Le misure minime previste dal disciplinare tecnico sono quasi totalmente implementate;• Solo poche minacce sono possibili.
Rischio «medio»:	<ul style="list-style-type: none">• Situazione con deficienze, tecniche oppure organizzative, note;• Molte misure minime previste dal disciplinare tecnico non sono implementate;• Esistono diverse minacce possibili e qualcuna anche probabile.
Rischio «alto»:	<ul style="list-style-type: none">• Situazione con deficienze diffuse e talvolta non completamente note;• Non è assegnata una responsabilità specifica per il controllo di quella problematica;• Le minacce sono probabili e si sono già concretizzate nel passato.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

4.2 SINTESI

Valutazione dei rischi per gli aspetti fisici:

Aree di rischio	Basso	Medio	Alto	Motivazione
Sede:				
Possibilità di intrusione nella sede		X		Ad uffici aperti locali sempre presidiati. Gli uffici sono però aperti al pubblico: il via vai di persone è inevitabile.
Possibilità di accedere senza controllo ai locali protetti	X			Ad uffici aperti locali sempre presidiati.
Allagamento	X			La zona non è soggetta ad allagamenti. Impianti e tubature recenti;
Incendio	X			Non vengono trattati materiali particolarmente infiammabili. Sono presenti degli estintori; esiste adeguata segnalazione.
Possibilità di provocare danni dall'esterno (sassate, bombe, traffico stradale)	X			Gli uffici sono al primo piano delle palazzine ASL;
Apparecchiature:				
Manomissione delle apparecchiature di trattamento dei dati	X			Ad uffici aperti locali sempre presidiati. Ad uffici chiusi impianto di allarme attivo.
Probabilità di guasti (per obsolescenza o per manutenzione carente)	X			Macchine mantenute con corretta frequenza.
Interruzioni di energia elettrica		X		Gruppi di continuità (bassa autonomia) presenti sulle macchine critiche;
Interruzioni di collegamenti telefonici		X		Sistema di centralino sottoposto a contratto di manutenzione.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

Analisi dei rischi per i programmi ed i dati:

Aspetti di rischio	Basso	Medio	Alto	Motivazione
Software:				
Possibilità di installare programmi non controllati	X			Sui client non è possibile installare software; gli utenti non hanno privilegi di amministrazione.
Accesso non autorizzato (inclusi terzi) ai programmi applicativi	X			Tutti gli accessi (sistemi operativi, applicazioni) sono protetti da password con scadenza ogni 90 giorni;
Correzioni per problemi di sicurezza non applicate	X			I sistemi sono configurati per ricevere ed installare gli aggiornamenti in modalità automatica;
Possibilità da parte dei virus di intaccare l' integrità del sistema	X			Aggiornamento automatico delle definizioni. Software attivo per scansione immediata di ogni file utilizzato.
Ripristino del servizio con il software aggiornato	X			Sistema operativo e programmi installati sono tutti contenuti in immagine su DVD per ripristino rapido funzionalità;
Dati:				
Accesso non autorizzato agli archivi	X			Le utenze sono configurate in base alle reali necessità di accesso ai dati;
Modifica o cancellazione errata di dati	X			Modifica o cancellazione errata di dati prevenuta dal sistema di accessi sopra descritto e da un sistema automatico di Backup;
Perdita (accidentale o dolosa) di dati	X			Perdita di dati prevenuta dal sistema di accessi s.d. e da un sistema automatico di Backup;
Intercettazione delle trasmissioni	X			E' installato (e correttamente aggiornato) un firewall;
Incapacità di ripristinare i dati dopo un evento che li abbia danneggiati	X			Perdita di dati prevenuta da un sistema automatico di Backup;

5. MISURE DI SICUREZZA

Per proteggere i dati personali dai rischi di cui al paragrafo precedente, vengono adottate le misure di sicurezza di seguito elencate.

Eventuali sospetti di incidente di sicurezza² devono essere immediatamente riportati all'Responsabile dei trattamenti informatici che, dopo l'analisi - secondo la gravità del problema - informa il Titolare.

Nota: Le misure di sicurezza sono suddivise nelle tre categorie della sicurezza: fisica, logica, delle comunicazioni.

5.1 MISURE PER LA SICUREZZA FISICA.

Per assicurare la sicurezza fisica dei locali ove vengono trattati dati personali, oltre alle misure previste da norme di legge (es. legge 81/2008) o da regole interne aziendali (protezione della sede), si programmano i seguenti controlli:

1. Le apparecchiature informatiche critiche per la sicurezza delle informazioni sono installate in locali chiusi a chiave al di fuori dell'orario di ufficio e quando non sono presenti persone per attività di manutenzione e di supporto.
2. Personale esterno all'azienda può accedere al locale e rimanervi per il tempo necessario a concludere l'attività richiesta (es. pulizia o manutenzione) solo con l'esplicita approvazione di chi consegna la chiave, che si accerta che all'interno non rimangano incustoditi supporti di registrazione di informazioni personali (es. tabulati, dischi, raccoglitori di documenti).
3. Eventuali nastri e dischetti, con copie degli archivi contenenti dati personali ed eventualmente anche dati sensibili, sono in locali chiusi.
4. Eventuali nastri e dischetti contenenti dati sensibili, quando non vengono più utilizzati per quel trattamento, devono essere distrutti fisicamente per evitare che possano essere recuperati i dati precedentemente registrati, anche se obsoleti.
5. Nastri e dischetti ottenuti per essere in grado di ripristinare la disponibilità dei dati dopo un evento disastroso (incendio delle apparecchiature, crollo del locale in cui sono installate, ecc.) sono accuratamente custoditi.
6. I locali con gli armadi usati per conservare documentazione cartacea devono essere muniti di idonea serratura e devono essere chiusi a chiave quando l'ufficio in cui sono ubicati non è presidiato. La chiave deve essere in possesso della persona cui è affidata la gestione di quella documentazione ed una copia è in possesso del Responsabile dei trattamenti per essere richiesta ed usata in caso di emergenza.

² In linea generale viene definito incidente di sicurezza qualunque evento inaspettato che comprometta o possa compromettere l'integrità, la riservatezza o la disponibilità delle informazioni

5.2 MISURE PER LA SICUREZZA LOGICA

Per assicurare la sicurezza logica delle informazioni, si programmano le seguenti misure e controlli:

1. Per utilizzare le stazioni di lavoro (terminali e PC) ed accedere alle applicazioni per il trattamento dei dati, gli incaricati devono usare una utenza (user-id) ed una password di autenticazione.
2. Le utenze sono strettamente individuali e vengono create dall' amministratore del sistema su richiesta del Responsabile dei trattamenti. Quando l' utenza è stata creata, viene comunicata all' interessato insieme alla password che consente il primo collegamento. All' atto del primo collegamento, la password deve essere modificata secondo le regole indicate successivamente.
3. L' utenza non deve essere assegnata, per nessun motivo, ad altro incaricato. Quando un incaricato lascia l' azienda, la sua utenza non può mai più essere utilizzata.
4. La misura di cui sopra deve essere applicata anche per le utenze create per consulenti e collaboratori esterni.
5. Almeno una volta l'anno, l' amministratore di sistema controlla se vi sono utenze non più usate da sei mesi e provvede a disattivarle. Prima di cancellare una utenza, verifica con il Responsabile dei trattamenti se permane la necessità che ha determinato la sua creazione e prende, con il suo accordo, le azioni opportune (cancellazione o mantenimento).
6. Se ragioni tecniche richiedono che utenze di supporto siano esentate dall' azione di cui al punto precedente, l' amministratore di sistema stila un elenco di tali utenze con le motivazioni del caso e lo fa controfirmare dal Responsabile dei trattamenti. Conserva tale documento per le revisioni annuali di cui in seguito.
7. Quando le motivazioni per cui una utenza è stata creata vengono meno (dimissioni, cambio attività, modifiche tecnologiche) l' amministratore di sistema provvede immediatamente a disattivare l' utenza. Con l' accordo del Responsabile dei trattamenti, l' utenza può essere mantenuta in essere (ma disattivata) fino a che non si siano concluse le attività di passaggio di consegne tra il precedente ed il nuovo incaricato; il tutto deve essere documentato. A questo punto viene cancellata, insieme con tutte le abilitazioni di corredo.
8. L' autenticazione dell' utenza avviene a mezzo di password. Questa è segreta e non deve essere comunicata ad altri né lasciata incustodita, per esempio scrivendola su agende o su foglietti di appunti. Un trattamento illecito fatto carpando la password ad un incaricato è comunque imputabile all' incaricato che non l' ha custodita correttamente.
9. Per assicurare la qualità della password, condizione essenziale per l' efficienza del sistema di sicurezza, questa deve soddisfare i seguenti requisiti:
 - avere una lunghezza di otto caratteri;
 - essere bloccata dopo 5 tentativi invalidi di inserimento;
 - non deve essere banale o facilmente indovinabile (es. non contenere dati facilmente riconducibili all'utente);
 - non essere uguale a una delle ultime 5 usate;
 - essere modificata almeno ogni 3 mesi.

[SS VAL SERIANA, per la messa in opera di questo punto, ha pianificato un intervento entro giugno 2011]

10. Quando una password viene dimenticata, oppure è bloccata perché inserita per 5 volte errata, l' amministratore di sistema si accerta che il richiedente sia l' incaricato che ne è legittimo proprietario e procede ad impostarne una nuova per il primo collegamento. Il richiedente è obbligato a questo punto ad impostarne una segreta secondo le regole definite sopra.
[SS VAL SERIANA, per la messa in opera di questo punto, ha pianificato un intervento entro giugno 2011]
11. Per superare situazioni di emergenza o per rispondere a richieste, legalmente motivate, di organismi investigativi dello Stato, con l' autorizzazione del Responsabile dei trattamenti la password di un utente può essere re-impostata per un accesso temporaneo. L' attività svolta deve essere documentata ed il legittimo proprietario della password deve essere informato appena possibile. Sarà sua cura a questo punto modificare la password usata per la situazione di emergenza ed impostarne una nuova, nota solo a lui.
12. Ogni incaricato ha l' obbligo di non lasciare incustodita la stazione di lavoro mentre è attivata una sessione di lavoro. Nel caso si debba assentare deve chiudere la sessione e, nel caso di PC, impedire l' accesso ad altri, per esempio utilizzando la password di power-on. Se poi non ritiene opportuno chiudere la sessione di lavoro, deve prevedere un programma di screen-saver con una password.
13. Utenza e password controllano il diritto di un incaricato di utilizzare una stazione di lavoro e di accedere ad una applicazione. Il trattamento dei dati avviene secondo un profilo di abilitazione rilasciato in accordo con le effettive necessità operative dell' incaricato ed in linea con le relative autorizzazioni.
14. Quando l'utente è un consulente od un collaboratore esterno, deve essere posta cura particolare nel definire il profilo di abilitazione, per evitare che possa accedere, per effetto di collegamento a profili generici validi per il personale interno, a dati e risorse non richieste per la specifica attività.
15. Il profilo di abilitazione viene impostato dall' amministratore di sistema secondo le richieste/autorizzazioni del Responsabile dei trattamenti. Copia dell' autorizzazione deve essere conservata dall' amministratore di sistema.
16. Una volta all' anno l' amministratore di sistema produce una lista delle utenze attivate ed i relativi profili di autorizzazione e la sottopone al Responsabile dei trattamenti. Questi verifica, per conoscenza diretta o consultando i referenti gerarchici degli incaricati, la correttezza delle autorizzazioni ed il permanere della necessità delle stesse. Quindi le conferma o richiede eventuali aggiornamenti all' amministratore di sistema, che archivia la documentazione.
17. Oggetto di questa verifica sono anche le utenze degli addetti alla gestione ed alla manutenzione degli strumenti di controllo, quindi tipicamente le utenze di amministratore di sistema e dei programmatori di supporto tecnico.
18. Almeno una volta all' anno l' amministratore di sistema deve aggiornare il software di base dei sistemi, applicando le correzioni per problemi di sicurezza rese disponibili dai produttori del software. Il mancato aggiornamento, per giustificato motivo, deve essere motivato e documentato dall' amministratore di sistema ed approvato dal Responsabile.

19. Almeno una volta all' anno il Titolare si accerta che le prescrizioni di questo documento siano tutte attivate e correttamente applicate. Se per qualcuna l' esito è negativo, si accerta delle motivazioni della mancata applicazione e definisce le azioni da intraprendere.

Alle applicazioni Web sono applicate le seguenti misure di protezione:

Nella pagina introduttiva, insieme alla illustrazione della policy per la privacy, vengono richiamate all' utente le misure per la sicurezza dell' account, in particolare la segretezza della password e le regole per il ripristino in caso di dimenticanza;

Per prevenire attacchi sistematici, è previsto il blocco temporaneo della sessione di un account per il quale siano segnalati più "log-in failed" e viene altresì segnalata una anomala situazione di rifiuto di connessione per password errata;

L' utente è in grado di modificare la password, indicando la vecchia, la nuova e la conferma della nuova;

Per il reset della password (per esempio perché dimenticata) vengono richieste alcune informazioni di controllo prima di inviare una e-mail con la nuova password; la nuova password deve essere modificata alla prima connessione;

Sul sistema le password sono memorizzate in forma crittografata;

La connessione a pagine web per l' immissione di dati personali e/o sensibili è protetta con SSL;

Prima di accedere a risorse protette, la sessione user deve essere autenticata, per evitare un accesso che by-passi il controllo;

All' utente è consentito e raccomandato il log-out dalla sessione, per evitare di lasciare attività in sospeso; in ogni caso è prevista un log-out automatico, a seguito di un periodo di inutilizzo del sistema;

L' uso dei cookies per facilitare l' accesso deve essere evitato, richiedere il log-in ad ogni sessione; se l' uso dei cookies non può essere evitato, limitare la validità temporale. Non memorizzare informazioni sensibili nei cookies. Marcare il cookie come sicuro, per evitare la sua trasmissione a pagine web non protette da SSL.

5.3 MISURE PER LA SICUREZZA DELLE COMUNICAZIONI.

Il risultato fondamentale da assicurare in tutte le fasi dell'erogazione dei servizi che coinvolgono dati sulla salute degli assistiti da S.S. VAL SERIANA consiste nella garanzia che nell'utilizzo dei Sistemi informativi, dei programmi e nell'impostazione delle metodologie di archiviazione e conservazione dei dati e dei supporti siano rispettati il principio di necessità, indispensabilità e pertinenza delle informazioni trattate. L'azienda deve quindi evitare procedure che consentano di identificare direttamente l'interessato o di raccogliere e gestire dati superflui o sovrabbondanti rispetto agli scopi del servizio. A questo fine si dovrà provvedere anche alla opportuna configurazione degli strumenti elettronici utilizzati.

E' necessario inoltre conformarsi alle disposizioni di cui al punto 24 del Disciplinare tecnico Allegato B al Codice Privacy che prescrivono agli Organismi operanti nel settore sanitario che il trattamento elettronico dei dati idonei a rivelare lo stato di salute venga effettuato mediante

tecniche di cifratura od utilizzazione di codici identificativi o altre soluzioni che consentano - alle persone autorizzate al trattamento - di identificare direttamente l'interessato solo in caso di stretta necessità. Tale misura di sicurezza deve essere estesa anche ai trattamenti effettuati con mezzi cartacei.

Quindi, nel trattamento cartaceo di compilazione ed archiviazione delle cartelle psico-sociali, si dovrà evitare di inserire nelle parti visibili qualunque indicazione relativa alla patologia dell'assistito o altri dati relativi allo stesso. Le cartelle dovranno essere conservate, come già espresso, in un archivio documentale chiuso a chiave.

5.4 MISURE PER LA SICUREZZA DELLE COMUNICAZIONI.

Per assicurare la sicurezza delle comunicazioni, sono previste le seguenti misure di controllo:

1. Sui computer è installato ed attivo un programma antivirus, che viene aggiornato automaticamente assieme al file dei virus (signature file).
2. L'accesso da e per l'esterno è controllato da un sistema firewall hardware sotto la responsabilità della ASL di Bergamo, che solo ha la possibilità di inserire/modificare le regole di controllo.
3. In caso di necessità la ASL di Bergamo ricava la lista delle regole/restrizioni del firewall e, se necessario, procede alle rettifiche opportune.

6. CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

A seguito di un atto o evento esterno che renda indisponibili i dati oggetto di trattamento, la disponibilità degli stessi deve essere ripristinata al più presto. Per i trattamenti di dati sensibili e giudiziari il limite massimo è stabilito essere di sette giorni. A tale scopo S.S. VAL SERIANA ha programmato le seguenti misure:

1. Esiste un processo che consente il salvataggio quotidiano degli archivi contenenti dati essenziali per le attività dell'azienda, ivi inclusi gli archivi contenenti dati personali e dati sensibili.
2. I dischi con le copie dei dati sono conservate a cura del Responsabile dei trattamenti informatici in locali chiusi a chiave.
3. Personale qualificato è sempre in grado di rendere disponibili i dati dopo una situazione di emergenza che abbia causato danni ingenti al sistema o alla rete.
4. Una volta ogni tre mesi viene condotta una prova di ripristino dei dati, partendo dalle copie, per verificare l'effettiva funzionalità della procedura predisposta. Il risultato del test viene archiviato.

7. INTERVENTI FORMATIVI

Per assicurare l'efficacia delle misure di sicurezza adottate dall'azienda è necessario che tutto il personale sia informato adeguatamente sulle stesse. Per questo scopo vengono previsti i seguenti interventi informativi/formativi:

1. il presente documento, con una nota di accompagnamento del Responsabile dei trattamenti, viene divulgato a tutti i dipendenti e collaboratori, che ne prendono visione; Il documento stesso viene reso disponibile per consultazione in formato elettronico;
2. il personale ha seguito il corso di formazione in aula su privacy e sicurezza, che consente di essere edotti sui principi e sulle regole in materia;
3. il personale neo-assunto deve seguire un breve corso di informazione sulla materia della privacy, in particolare sugli aspetti di sicurezza. A cura del Responsabile dei trattamenti, o suo delegato, viene illustrato il presente documento ed i dettagli delle misure previste;
4. in occasione di aggiornamenti tecnologici o dell'individuazione di nuove aree di rischio, il Titolare, con il supporto del Responsabile per i trattamenti informatici, deve prevedere opportune sessioni informative degli incaricati, che a sua discrezione possono assumere le forma di corso apposito o di intervento in riunione di reparto. In ogni caso, deve essere redatto un verbale con l'indicazione dei partecipanti e degli argomenti trattati.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

8. TRATTAMENTI AFFIDATI ALL' ESTERNO

Per tutte le attività di trattamento (diretto e indiretto) affidate ad Enti esterni (fornitori di servizi, consulenti, programmatori, ecc.) è richiesto che vengano applicate le stesse misure di sicurezza applicate all' interno di S.S. VAL SERIANA. Perciò, in queste casistiche, è necessario che nei contratti stipulati con tali soggetti si valuti l'opportunità di inserire le seguenti clausole (solo se pertinenti):

1. il contraente dichiara 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 (D.lgs 196/2003);
2. dichiara di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. riconosce il diritto del committente a verificare, previo congruo preavviso, l'applicazione delle norme di sicurezza adottate.

Inoltre si rammenta che al termine di eventuali attività che comportino l' installazione o la modifica di uno strumento di controllo della sicurezza, l'Ente esterno è tenuto a rilasciare dichiarazione scritta che l' intervento effettuato è conforme alla normativa esistente.

Da parte sua S.S. VAL SERIANA, se necessario, fornirà al contraente un elenco delle misure di sicurezza previste per lo specifico trattamento, estraendole dal presente documento.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

9. NORME PER GLI INCARICATI DEL TRATTAMENTO

9.1 NORME DI CARATTERE GENERALE

- Il trattamento di dati personali deve avvenire da parte degli Incaricati solo se richiesto dal Responsabile di quel trattamento;
- l'uso delle apparecchiature informatiche che contengono dati personali o aziendali è permesso solo per svolgere le attività previste nelle istruzioni scritte impartite agli Incaricati;
- copie di dati personali su supporti amovibili (a.e CD-Rom, DVD, memory pen USB) sono permesse solo se parte del trattamento. In ogni caso tali supporti non devono mai essere lasciati incustoditi;
- i raccoglitori con documenti cartacei contenenti dati personali devono essere riposti, dopo il loro utilizzo, in armadi chiusi;
- al termine dell'orario di lavoro il dipendente, nell'abbandonare il proprio posto di lavoro, deve lasciare la scrivania sgombra e con tutti i cassette/armadi chiusi a chiave;
- in caso si constati o si sospetti un incidente di sicurezza, secondo le procedure in vigore, deve essere data immediata comunicazione al Responsabile dei trattamenti informatici e/o al Responsabile del trattamento coinvolto;
- queste norme si applicano anche ai terzi autorizzati ad accedere dall'esterno (fornitori, consulenti ecc.)

9.2 COMPILAZIONE DELLE CARTELLE PSICO-SOCIALI

Nel trattamento cartaceo di compilazione ed archiviazione delle cartelle psico-sociali, si dovrà prevedere una cover esterna in cui emerga solo il dato anagrafico dell'assistito, al fine di evitare che in prima pagina compaiano lo stato di salute o il motivo della richiesta dell'assistito.

9.3 USO DELLE WORKSTATION

Ogni dipendente è responsabile di fornire il proprio contributo al fine di minimizzare la possibilità che i dati personali e aziendali contenuti nella propria workstation, o trattati tramite la workstation, siano esposti a rischi di sicurezza.

A tale scopo, è attiva sulla workstation una password di accesso, che assicura che solo il titolare possa accedere ai dati registrati sulla stessa. Inoltre devono essere seguite le regole di seguito descritte.

Se si lascia incustodita la scrivania durante l'orario di lavoro:

- spegnere la workstation o se l'apparecchiatura deve restare accesa, attivare una password (keyboard o screen lock);
- assicurare i portatili con gli appositi strumenti o riporli in un armadio/cassetto chiusi a chiave.

Al termine della giornata di lavoro:

- spegnere la workstation o attivare una password (keyboard o screen lock);
- se si dispone di un portatile riporlo sotto chiave.

9.4 STAMPANTI E FAX

- Gli incaricati al trattamento devono controllare il processo di stampa dei documenti al fine di ridurre al minimo il rischio che persone non autorizzate possano accedere agli stessi;
- la stampa di documenti contenenti dati personali sensibili o aziendali riservati deve, pertanto, essere effettuata su stampanti o fax posti in locali ad accesso controllato o su stampanti presidiate dall'Incaricato durante le fasi di stampa;
- se la trasmissione di dati idonei a rivelare lo stato di salute di un assistito avviene a mezzo fax, occorre :
 - i) aggiungere alla comunicazione una cover, che non renda immediatamente identificabile lo stato di salute dell'assistito;
 - ii) concordare – ove possibile - con il ricevente che i fax siano prelevati solo da personale autorizzato.

9.5 USO DELLE PASSWORD [A REGIME DA GIUGNO 2011]

La password è un elemento fondamentale della sicurezza delle informazioni. La password identifica in modo univoco l'utente del computer e dei servizi informatici. Per la protezione dei dati personali è essenziale che la password sia mantenuta riservata e non comunicata ad altri. Le regole base da rispettare sono:

- la lunghezza minima della password è di 8 caratteri;
- la password deve essere mantenuta riservata e non comunicata ad altri utenti. Se, eccezionalmente, dovesse essere necessario fornirla, in caso di emergenza, ad altra persona, va cambiata subito dopo;
- la password non deve essere banale o facilmente individuabile. A tale scopo devono essere seguite le regole di composizione emesse dai Sistemi Informativi;
- non contenere l' User-ID, o il proprio nome, come parte della password;
- la password deve essere cambiata almeno ogni 90 giorni;
- se si accede dall'esterno non utilizzare per l'accesso alla rete la stessa password valida per l'accesso alle banche dati.

Nota: è responsabilità dell'utente rispettare queste regole anche se la tecnologia non le rende obbligatorie sulla propria workstation.

9.6 INTERNET

Nel caso si utilizzi la rete Internet per collegarsi con altre organizzazioni e si trasmettano dati personali, bisogna tenere presente le seguenti avvertenze:

- Internet è usato da milioni di persone nel mondo. Non di tutte possiamo fidarci;
- ogni informazione trasmessa può essere letta da un elevato numero di persone sconosciute;
- non trasmettere all'esterno dati personali sensibili o aziendali riservati se non resi inintelligibili;
- non trasmettere posta elettronica interna della S.S. VAL SERIANA tramite Internet, ma usare il sistema ufficiale;
- non è permesso prelevare software da Internet senza l'autorizzazione del Responsabile dei Trattamenti Informatici;
- non prelevare o inserire in Internet materiale inappropriato, offensivo o pregiudizievole per altre persone o organizzazioni.

Se ritenuto opportuno, per una maggior consapevolezza, le regole di comportamento per l'utilizzo di Internet possono essere definite in modo analitico in un documento da rendere disponibile ad ogni dipendente, sia in forma di pieghevole, sia in formato elettronico su intranet.

10. VERIFICA DELLO STATO DELLA SICUREZZA

10.1 VERIFICHE DELL' ARCHITETTURA DI SICUREZZA

Almeno ogni 6 mesi il Responsabile dei trattamenti informatici deve effettuare controlli per verificare che gli elementi chiave, ai fini della sicurezza dei sistemi, siano integri.

I controlli per i sistemi critici (contenenti applicazioni su dati sensibili, aziendali riservati, firewall, ecc.) devono avere una frequenza trimestrale.

Le verifiche devono comprendere:

- i parametri del sistema di controllo accessi;
- la lista delle persone con autorità di sistema o di sicurezza;
- i parametri di sicurezza dei sistemi operativi;
- l'aggiornamento del programma antivirus.

I controlli effettuati ed il loro esito, nonché le azioni pianificate per correggere eventuali deviazioni, devono essere riportati in un apposito verbale.

10.2 PROCESSO DI PREVENZIONE E ALLARME (ALERT)

Il Responsabile del trattamento Informatico deve predisporre un programma che permetta di anticipare i possibili problemi legati alla sicurezza delle informazioni.

Con cadenza annuale, o in occasione di significativi cambiamenti alle architetture informatiche, deve essere effettuata una valutazione di rischio.

Deve essere mantenuto un collegamento con il CERT, o altra istituzione che abbia le stesse finalità, per essere informati riguardo alle esposizioni di sicurezza dei principali prodotti software utilizzati.

Nel caso siano segnalate dal CERT, o altra istituzione che abbia le stesse finalità, esposizioni definite ad alto rischio, sui prodotti installati, deve essere subito valutata l'opportunità di intervento.

10.3 ATTACCHI SISTEMATICI

Deve essere attivato almeno un sistema che permetta di rilevare quando il numero dei tentativi non riusciti di login superano una determinata soglia di pericolo oltre il quale si deve indagare su possibili attacchi.

[SS VAL SERIANA, per la messa in opera di questo punto, ha pianificato un intervento entro dicembre 2011]

10.4 INCIDENTI DI SICUREZZA

In linea generale viene definito *incidente di sicurezza* qualunque evento inaspettato che

riguardi l'integrità, la riservatezza o la disponibilità delle informazioni. È compito del Responsabile dei trattamenti informatici rilasciare una procedura che definisca una articolazione degli incidenti per gravità e la relativa gestione.

Una appropriata gestione degli incidenti è fondamentale per tenere sotto controllo questo fenomeno e mettere in atto le opportune contromisure per ridurli.

10.5 GESTIONE DEI LOG

L'Amministratore di sistema deve predisporre un processo per garantire che i log elencati siano attivi e protetti da accessi non autorizzati. I log devono essere conservati per almeno 2 mesi.

- Se il sistema operativo lo consente, tutti i tentativi di login - sia che abbiano avuto successo sia che siano stati rifiutati - devono essere registrati;
- se il sistema di controllo accessi lo consente, il Responsabile del trattamento può chiedere che siano registrati gli accessi alle singole risorse;
- se il sistema operativo lo consente, le attività svolte dalle persone con autorità di sistema o di amministrazione della sicurezza devono essere registrate.
- la lista dei login invalidi è fornita da parte degli Amministratori di sistema su richiesta del Responsabile del trattamento;
- le registrazioni che compongono i log, in quanto dati personali, devono essere oggetto di uno specifico trattamento che ne preveda l'utilizzo solo per finalità di sicurezza in caso di pericolo o di incidente.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

11. DISPONIBILITÀ, DA PARTE DELL'AZIENDA, DEGLI STRUMENTI E DEI DATI AFFIDATI AL DIPENDENTE

Per garantire al Titolare, in caso di assenza dell'incaricato e per urgenti necessità, l'accesso agli strumenti ed ai dati ivi contenuti devono essere rispettate le seguenti modalità:

- solo il Responsabile dei trattamenti possono autorizzare un altro incaricato a sostituirsi alla persona assente e ad utilizzare la sua User-ID ed il relativo profilo di accesso;
- solo il Responsabile dei trattamenti possono autorizzare gli Amministratori di sistema a fornire all'incaricato autorizzato le credenziali di accesso;
- se il sistema lo permette, per fornire le nuove credenziali, si deve utilizzare la stessa metodologia usata per il reset delle password. In tal modo viene mantenuta la segretezza delle credenziali della persona assente;
- le autorizzazioni di accesso devono risultare da appositi documenti conservati dagli Amministratori di sistema ed essere a disposizione del Titolare per i necessari controlli e verifiche;
- a cura dell'Amministratore del sistema coinvolto, devono essere attivate, limitatamente al periodo di tempo necessario, le registrazioni dei log delle attività della User-Id interessata;
- a cura del Responsabile di trattamento, la persona assente, deve essere informata al suo rientro, su quanto avvenuto;
- il Responsabile dei trattamenti informatici deve definire e mantenere aggiornata una specifica procedura che regola le modalità sopra descritte.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

12. CONTROLLI E AUDIT

Almeno annualmente il Titolare fa verificare con appropriati controlli audit l'aderenza dello stato della sicurezza al presente DPS.

Al termine dell'audit l'Amministratore di sistema o il Responsabile interessato, se sono riscontrate deviazioni, deve formulare un piano che preveda il rientro nel più breve tempo possibile.

Situazioni di non aderenza, per periodi superiori a 6 mesi, possono essere accettati solo con l'esplicita autorizzazione scritta del Responsabile di riferimento il quale ha comunque l'obbligo di informare per iscritto il Titolare.

È compito del Responsabile dei trattamenti informatici effettuare verifiche periodiche sullo stato della sicurezza in azienda anche in relazione ad eventuali outsourcer esterni che trattano dati personali o aziendali riservati.

Un rapporto sullo stato della sicurezza, anche in base agli esiti dei self assessment, deve essere predisposto almeno semestralmente e inviato al Titolare ed al Responsabile.

È compito dei singoli Responsabili e degli Amministratori di sistema, nell'ambito delle proprie responsabilità, effettuare delle verifiche periodiche (sulla base di liste di controllo) e predisporre adeguati piani correttivi in caso di scostamenti.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

13. REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente DPS è valido per un anno. Trascorso tale termine deve essere oggetto di revisione, a cura del Responsabile dei trattamenti informatici, per adeguarlo ad eventuali variazioni del livello di rischio cui sono soggetti i dati personali e ad eventuali modifiche della tecnologia informatica. In ogni caso il DPS deve essere aggiornato entro il 31 marzo di ogni anno.

Nell'attesa dell'adeguamento conservano validità le istruzioni in vigore.

Data: 31 Marzo 2011

IL TITOLARE

Firma del Legale Rappresentante: _____