

**ESTRATTO DEL
DOCUMENTO
PROGRAMMATICO
sulla SICUREZZA
dei DATI PERSONALI**

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.....	3
1.1 SCOPO DEL DOCUMENTO	3
1.2 PRINCIPI GENERALI	3
1.3 DEFINIZIONI.....	3
2. MISURE DI SICUREZZA.....	6
2.1 MISURE PER LA SICUREZZA FISICA.....	6
2.2 MISURE PER LA SICUREZZA LOGICA	6
2.3 MISURE PER LA SICUREZZA DELLE COMUNICAZIONI.	9
3. CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI	10
4. INTERVENTI FORMATIVI	11
5. TRATTAMENTI AFFIDATI ALL' ESTERNO	12
6. NORME PER GLI INCARICATI DEL TRATTAMENTO	13
6.1 NORME DI CARATTERE GENERALE.....	13
6.2 COMPILAZIONE DELLE CARTELLE PSICO-SOCIALI.....	13
6.3 USO DELLE WORKSTATION.....	13
6.4 STAMPANTI E FAX.....	14
6.5 USO DELLE PASSWORD	14
6.6 INTERNET	14
7. VERIFICA DELLO STATO DELLA SICUREZZA.....	16
7.1 VERIFICHE DELL' ARCHITETTURA DI SICUREZZA.....	16
7.2 PROCESSO DI PREVENZIONE E ALLARME (ALERT).....	16
7.3 ATTACCHI SISTEMATICI	16
7.4 INCIDENTI DI SICUREZZA.....	16
7.5 GESTIONE DEI LOG.....	17
8. DISPONIBILITÀ, DA PARTE DELL'AZIENDA, DEGLI STRUMENTI E DEI DATI AFFIDATI AL DIPENDENTE	18
9. CONTROLLI E AUDIT.....	19
10. REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA.....	20

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 la SOCIETA' SERVIZI SOCIOSANITARI VAL SERIANA (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 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.

1.3 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. MISURE DI SICUREZZA

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

Eventuali sospetti di incidente di sicurezza¹ devono essere immediatamente riportati all'Responsabile dei trattamenti informatici che, dopo l'analisi - secondo la gravità del problema - informa il Titolare.

2.1 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 626) 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 custoditi in armadi 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 custoditi in cassetta di sicurezza.
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.

2.2 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.

¹ 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

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. Ogni mese 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 carpendo 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;
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.
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. Utente 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, preferibilmente all'atto della stesura della relazione accompagnatoria del bilancio di esercizio, 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.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

2.3 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 dell'amministratore di sistema, che solo ha la possibilità di inserire/modificare le regole di controllo.
3. Una volta ogni sei mesi l'amministratore di sistema ricava la lista delle regole/restrizioni del firewall e verifica la corrispondenza con quanto risulta dalla documentazione in suo possesso. Se necessario procede alle rettifiche opportune ed archivia il documento dopo averlo firmato.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

3. 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 settimanale degli archivi contenenti dati essenziali per le attività dell'azienda, ivi inclusi gli archivi contenenti dati personali e dati sensibili.
2. Nastri e dischi con le copie dei dati sono conservate a cura del Responsabile dei trattamenti informatici in armadi ignifughi, chiusi a chiave.
3. Nel luogo di conservazione delle copie, deve essere custodita una breve procedura operativa che descriva i passi da eseguire per rendere disponibili i dati dopo una situazione di emergenza che abbia causato danni ingenti al sistema o alla rete. Scopo della procedura è di fornire gli elementi necessari per completare l'operazione in situazione di emergenza, eventualmente anche con il coinvolgimento di persone non completamente aggiornate sulle operazioni abituali.
4. Una volta all'anno deve essere condotta una prova di ripristino dei dati, partendo dalle copie, per verificare la fattibilità della procedura predisposta. Il risultato del test deve essere archiviato con la procedura stessa.

4. 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 deve seguire un corso di formazione 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]

5. 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]

6. NORME PER GLI INCARICATI DEL TRATTAMENTO

6.1 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 sono permesse solo se parte del trattamento. In ogni caso tali supporti devono avere un'etichetta che li identifichi e 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 cassetti/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.)

6.2 COMPILAZIONE DELLE CARTELLE PSICO-SOCIALI

Nel trattamento cartaceo di compilazione delle cartelle psico-sociali, si dovrà prevedere un format che nella copertina esterna indichi i soli dati anagrafici dell'assistito, al fine di evitare che in prima pagina compaiano lo stato di salute o il motivo della richiesta di intervento.

6.3 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 richiesto che venga attivata sulla workstation la password di accensione, 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.

6.4 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.

6.5 USO DELLE PASSWORD

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.

6.6 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.

[PARTE DI PAGINA LASCIATA INTENZIONALMENTE IN BIANCO]

7. VERIFICA DELLO STATO DELLA SICUREZZA

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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]

8. 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]

9. 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]

10. 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: 31/03/05

IL TITOLARE

Firma del Legale Rappresentante: Il Presidente
F.to Sig.ra Luiselli Manuella