

CONSORZIO UNIVERSITARIO PER L'ATENEO DELLA SICILIA OCCIDENTALE E DEL BACINO DEL MEDITERRANEO

Via Pier Santi Mattarella, n. 188, 91100-Trapani (TP)
Via Quarto dei Mille, n. 6 90100 - Palermo

Si richiede l'apposizione del timbro postale per la data certa.
Il presente documento redatto in corpo unico è composto
da n. 34 pagine

DECRETO LEGISLATIVO 196/2003 "Codice in materia di protezione dei dati personali"		DATA ULTIMA REVISIONE
ALLEGATO N°	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA <small>(In ottemperanza a quanto previsto dal Disciplinare Tecnico - Allegato B)</small>	Marzo 2011
1		TOTALE PAGINE 34

Il Titolare del Trattamento

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 1 di 34

INDICE

1. Premessa	3
2. Principali Riferimenti Legislativi	3
3. Finalità e composizione del DPSS	3
4. Campo di applicazione	7
5. Identificazione delle Risorse da Proteggere	8
5.1. Luoghi Fisici	8
5.2. Risorse Hardware	10
5.3. Risorse Software	16
5.4. Banche dati ed elenco dei Trattamenti di Dati Personali	17
6. Elenco sedi ed uffici nei quali avviene il trattamento dei dati	20
7. Elenco cariche dei soggetti che effettuano il trattamento dei dati	20
8. Analisi dei Rischi	23
8.1. Analisi dei Rischi sulle Aree e sui Locali	24
8.3. Analisi dei Rischi sulle Risorse Software	24
9.1. Misure di Sicurezza di tipo Fisico adottate	27
9.2. Misure di Sicurezza di tipo Logico adottate	28
9.4. Misure adottate per garantire l'integrità e la disponibilità dei dati	30
10. Criteri e modalità di ripristino dei dati	30
11. L'affidamento di dati personali all'esterno	31
12. Piano di Verifica delle Misure adottate	32
13. Piano di Formazione degli Incaricati	32
14. Dichiarazioni d'impegno e firma	34

1. Premessa

Il Codice sulla privacy (D.lgs.vo 196/2003) impone a chiunque tratta informazioni relative ad altre persone, imprese, enti od associazioni di rispettare alcuni principi fondamentali a garanzia della riservatezza dei dati stessi.

Il Codice prescrive precisi obblighi e comportamenti da attuare nel trattare i dati; questi obblighi sono sanzionati anche penalmente: è necessario, pertanto, procedere all'adeguamento dell'organizzazione aziendale al fine di rispettare gli obblighi imposti dal Codice.

Con il presente “Documento Programmatico Sulla Sicurezza” si definisce, ai sensi delle disposizioni di cui all'Articolo 34 del Decreto Legislativo n. 196 del 30 giugno 2003 e del relativo Disciplinare Tecnico (allegato B), il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato da UNISOM - CONSORZIO UNIVERSITARIO PER L'ATENEO DELLA SICILIA OCCIDENTALE E DEL BACINO DEL MEDITERRANEO con sede legale in Trapani (TP) in Via Pier Santi Mattarella, n. 188, sede amministrativa in Trapani in Via Colonnello Romey, n. 15, e sede periferica in Palermo in Via Quarto dei Mille, n. 20, - P.IVA: 02041460813 (nel seguito del documento indicato come Titolare e abbreviato con UNISOM), nella sua attività di servizi inerenti l'organizzazione e la formazione Professionale e l'attivazione di corsi di laurea.

2. Principali Riferimenti Legislativi

Le disposizioni di legge principali concernenti la corretta gestione di sistemi informatici sono:

D. Lgs. 29 dicembre 1992, n. 518 – Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore.

Legge 23 dicembre 1993, n. 547 – Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.

D. Lgs. 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali. – Disciplinare Tecnico (allegato B)

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

3. Finalità e composizione del DPSS

Il presente Documento Programmatico Sulla Sicurezza trae la propria origine dalle disposizioni di cui al Decreto Legislativo n. 196 del 30 giugno 2003 e relativo Disciplinare Tecnico (allegato B), che per definire le politiche di sicurezza in materia di trattamento dei dati personali nonché i criteri tecnico-organizzativi per la loro attuazione, così dispongono:

Decreto Legislativo n. 196/2003

Art. 33 (Misure minime)

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo, o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34 (Trattamenti con strumenti elettronici)

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 3 di 34

- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza;
- h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Art. 35 (Trattamenti senza l'ausilio di strumenti elettronici)

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- b) previsione di procedure per un'adeguata custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 36 (Adeguamento)

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata e conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso a uso esclusivo dell'incaricato eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è 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; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 4 di 34

sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito, esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con le quali il titolare 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. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando, preventivamente, per iscritto i soggetti incaricati della loro custodia, i quali devono informare, tempestivamente, l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di accesso di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico, con cadenza almeno annuale, dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi, di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno il titolare di un trattamento di dati sensibili o di dati giudiziari redige, anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

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

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

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 5 di 34

- 19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché, la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità;
- 19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
- 19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali;
- 19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- 19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi e compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati, con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare, che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 6 di 34

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico, con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione, al termine delle operazioni affidate, in maniera che ad essi non accedano persone prive di autorizzazione.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Con l'intento di recepire completamente lo spirito con cui è stata varata la norma, si è elaborato il presente Documento Programmatico Sulla Sicurezza (nel seguito denominato più semplicemente DPSS), al fine di garantire la protezione, l'integrità e la conservazione di ogni singolo dato personale trattato.

Il documento procede, innanzi tutto, all'**Identificazione delle Risorse da proteggere**, risorse che in diverso modo operano o comunque svolgono un ruolo significativo nei processi di trattamento dei dati personali, si passa poi all'analisi ed all'elenco dei trattamenti e quindi alla distribuzione dei compiti e delle responsabilità nell'ambito della struttura organizzativa. Poi, tramite l'**Analisi dei Rischi**, sono state analizzate le minacce e le vulnerabilità a cui le risorse sono sottoposte, in modo da potere valutare gli elementi che possono insidiare la protezione, l'integrità e la conservazione di ogni singolo dato personale trattato.

Valutati i rischi, si è redatto un **Piano di Sicurezza** tramite il quale si è provveduto a definire l'insieme delle misure fisiche, logiche ed organizzative adottate per tutelare le strutture e le risorse preposte al trattamento dei dati e le misure da adottare per garantire l'integrità e la disponibilità dei dati stessi.

Inoltre, è stato definito un **Piano di Verifiche** delle misure adottate tramite il quale si provvederà ad accertare, periodicamente, la bontà delle misure individuate e ad apportare gli accorgimenti che si riveleranno necessari ed opportuni.

Parallelamente alla stesura del **Piano di Verifiche** è stato redatto un **Piano di Formazione degli Incaricati** tramite il quale si renderanno edotti gli incaricati del trattamento dei rischi e dei modi per prevenire i danni.

Il Documento Programmatico sulla Sicurezza, va aggiornato annualmente entro ogni 31 marzo.

4. Campo di applicazione

Il **Documento Programmatico Sulla Sicurezza adottato da UNISOM** e del quale si richiamano tutte le definizioni e disposizioni, definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico Sulla Sicurezza riguarda tutti i dati personali:

- ▷ Sensibili
- ▷ Giudiziari
- ▷ Comuni

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali per mezzo di:

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 7 di 34

- ▷ Strumenti elettronici di elaborazione
- ▷ Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Il Documento Programmatico Sulla Sicurezza deve essere conosciuto ed applicato da tutti i componenti e collaboratori dell' **UNISOM**.

5. Identificazione delle Risorse da Proteggere

Le risorse coinvolte nel trattamento dei dati personali sono state divise nelle seguenti categorie:

- ▶ **Luoghi Fisici:** Sono stati analizzati tutti i luoghi ove fisicamente si svolge il trattamento dei dati o si trovano i sistemi di elaborazione o i luoghi ove si conservano i dati;
- ▶ **Risorse hardware:** Sono state analizzate le apparecchiature elettroniche che sono coinvolte nelle operazioni di trattamento.
- ▶ **Risorse software:** Sono stati analizzati i software applicativi mediante i quali vengono effettuati i trattamenti automatizzati;
- ▶ **Banche Dati:** Sono stati analizzati tutti gli archivi contenenti dati personali trattati dal Consorzio siano essi in formato elettronico che in formato cartaceo.

5.1. Luoghi Fisici

I luoghi fisici in cui avvengono i trattamenti sono i seguenti:

SCHEDA RILEVAZIONE LUOGHI FISICI	
Città:	Trapani (TP) – Palermo (PA)
Indirizzo Sede legale:	Via Pier Santi Mattarella, n. 188 – Trapani (TP)
Indirizzo Sede amministrativa:	Via Colonnello Romey, n. 15 91100 (TP) Via G. B. Fardella, n. 130 – 91100 (TP)
Indirizzo Sede periferica:	Via Quarto dei Mille, n. 6 – Palermo (PA)
Descrizione Sede:	Nelle sedi amministrative risultano depositate rispettivamente, nella Via Colonnello Romey, le scritture contabili tenute dal Consulente aziendale Studio S. Montemario e nella Via G.B. Fardella, le documentazioni attinenti i dipendenti tenute dal consulente del lavoro Maria Stella Grammatico. Nella sede di Via Pier Santi Mattarella, n. 188, l'accesso è protetto da un portone con serratura. Il Consorzio usufruisce di n. 5 locali ad uso ufficio. La sede è dotata di estintori e l'impianto elettrico è a norma. Sono presenti cassette e armadi sia di tipo metallico che di tipo legno dotati di serratura. Sono presenti i PC n. 01, 02, 03 e 04. In via Quarto dei Mille, n. 20 l'accesso è garantito da un portone blindato. Il Consorzio ha provveduto agli adempimenti previsti dal D.Lvo 81/08; ne segue che sono presenti gli estintori.

LOCALI		
Descrizione e posizione	Uso	Dispositivo di protezione Note
Locali di Via P.S. Mattarella, n. 188	Sede Legale	Sono presenti gli elaboratori nn. PC 01, PC 02, PC 03, PC04; sono presenti: fax, fotocopiatore, stampante e scanner, armadi con e senza serratura, cassette con serratura e scaffalature. Sono inoltre presenti n. 4 gruppi di continuità. Il sistema di connettività è l' ADSL Alice.
Locali di Via Quarto dei Mille, n. 6	Ufficio	Sono presenti: elaboratori, fax, fotocopiatore, stampanti e scanner. La società gestisce i sistemi di formazione anche a distanza. La sede è dotata di due gruppi di continuità e di un Firewall router Alice. I PC 05 e 06 sono client non in rete; il sistema di connettività è l' ADSL Alice in Wirelles.

5.2. Risorse Hardware

Le risorse hardware utilizzate per trattare i dati personali sono analizzate nelle seguenti schede riepilogative:

SCHEDE RILEVAZIONE RISORSE HARDWARE N. 1 (in affitto dalla DEF di Dario Cardella)	
Codice:	PC 1
Modello:	Assemblato
Sistema Operativo:	Windows XP Professional S.P.2
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico:
Dislocazione:	Locale n. Via P.S. Mattarella, n. 188
Operatore:	

DISPOSITIVI DI PROTEZIONE	
Presenza di Password:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Note:
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: AVIRA Note:
Firewall:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Di Sistema Note:
Gruppo di Continuità:	<input checked="" type="checkbox"/> No <input type="checkbox"/> Si

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI	
Componente	Descrizione
Supporti di memorizzazione	Disco rigido da Gb Floppy, Lettore CD.
Connessione Internet	Connettività ADSL TELECOM ALICE

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 2 (in affitto dalla DEF di Dario Cardella)

Codice:	PC 2
Modello:	Assemblato
Sistema Operativo:	Windows XP Professional S.P.2
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico:
Dislocazione:	Locale n. Via P.S. Mattarella, n. 188
Operatore:	

DISPOSITIVI DI PROTEZIONE

Presenza di Password:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Note:
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: AVIRA Note:
Firewall:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Di Sistema Note:
Gruppo di Continuità:	<input checked="" type="checkbox"/> No <input type="checkbox"/> Si

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
Supporti di memorizzazione	Disco rigido da Gb Floppy, Lettore CD.
Connessione Internet	Connettività ADSL TELECOM ALICE

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 3 (in affitto dalla DEF di Dario Cardella)

Codice:	PC 3
Modello:	Assemblato
Sistema Operativo:	Windows XP Professional S.P.2
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico:
Dislocazione:	Locale n. Via P.S. Mattarella, n. 188
Operatore:	

DISPOSITIVI DI PROTEZIONE

Presenza di Password:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Note:
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto:AVIRA Note:
Firewall:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Di Sistema Note:
Gruppo di Continuità:	<input checked="" type="checkbox"/> No <input type="checkbox"/> Si

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
Supporti di memorizzazione	Disco rigido da Gb Floppy, Lettore CD.
Connessione Internet	Connettività ADSL TELECOM ALICE

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 4 (in affitto dalla DEF di Dario Cardella)

Codice:	PC 4
Modello:	Assemblato
Sistema Operativo:	Windows XP Professional S.P.3
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico:
Dislocazione:	Locale n. Via P.S. Mattarella, n. 188
Operatore:	

DISPOSITIVI DI PROTEZIONE

Presenza di Password:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Note:
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: AVIRA Note:
Firewall:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Di Sistema Note:
Gruppo di Continuità:	<input checked="" type="checkbox"/> No <input type="checkbox"/> Si

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
Supporti di memorizzazione	Disco rigido da Gb Floppy, Lettore CD.
Connessione Internet	Connettività ADSL TELECOM ALICE

SCHEDE RILEVAZIONE RISORSE HARDWARE N. 5	
Codice:	PC 5
Modello:	ASSEMBLATO Intel Celeron 4 Gb
Sistema Operativo:	WINDOWS XP PROFESSIONAL S.P. 3
Licenza n°:	FB49T-PYWK6-X3BHD-7GPTB-J7CX8
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico:
Dislocazione:	Locale n. Via Quarto dei Mille 6
Operatore:	

DISPOSITIVI DI PROTEZIONE	
Presenza di Password:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Note:
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Comodo Antivirus Note:
Firewall:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: DI SISTEMA Note:
Gruppo di Continuità:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si TRUST PW 4080T

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI	
Componente	Descrizione
Supporti di memorizzazione	HARD DISK DA 500 GB
Connessione Internet	Connettività ADSL Alice

SCHEDE RILEVAZIONE RISORSE HARDWARE N. 6	
Codice:	PC 6
Modello:	ASSEMBLATO Intel Celeron 4 Gb
Sistema Operativo:	WINDOWS XP PROFESSIONAL S.P. 3
Licenza n°:	F4P64-MBBKG-MBBKG-KK74D-8RQ73-XB4GJ
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico:
Dislocazione:	Locale n. Via Quarto dei Mille, n. 6.
Operatore:	

DISPOSITIVI DI PROTEZIONE	
Presenza di Password:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Note:
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Comodo Antivirus Note:
Firewall:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: DI SISTEMA
Gruppo di Continuità:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si TRUST

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI	
Componente	Descrizione
Supporti di memorizzazione	HARD DISK DA 500 GB
Connessione Internet	Connettività ADSL Alice

5.3. Risorse Software

I software applicativi utilizzati per trattare i dati personali sono analizzati nelle seguenti schede riepilogative:

SCHEDA RILEVAZIONE RISORSE SOFTWARE N. 01	
Nome Software:	Windows XP 2002
Categoria:	<input type="checkbox"/> Sistema Operativo <input type="checkbox"/> Software di Base <input type="checkbox"/> Software Applicativo
Breve Descrizione:	
Versione:	
Presenza di Password:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Note:
Frequenza Aggiornamenti	
Codice delle Risorse Hardware su cui è installato il Software:	

5.4. Banche dati ed elenco dei Trattamenti di Dati Personali

Gli archivi e le banche dati contenenti i dati personali trattati sono i seguenti:

- ▶ BANCA DATI CLIENTI;
- ▶ BANCA DATI FORNITORI;

SCHEMA RILEVAZIONE BANCHE DATI N. 01	
Codice:	BD01
Descrizione:	BANCA DATI CLIENTI. In questa banca dati sono conservati i dati dei clienti del Consorzio.
Tipologia risorsa:	[x] Archivio Elettronico [X] Archivio Cartaceo
Ubicazione Banca Dati	Cartacea: Via P.S. Mattarella, n. 188, Via Quarto dei Mille, n. 20 Elettronica: Via P.S. Mattarella, n. 188, Via Quarto dei Mille, n. 20
Incaricati della Raccolta	
Risorse Hardware su cui è ospitata:	
NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO	
Dato	Natura del Dato
Nominativo, Indirizzo, Numero di telefono, telefax, etc	Non sensibile
Numero Carta d'identità, Codice fiscale, Partita IVA,	Non sensibile
Curriculum vitae, Curriculum lavorativo, Curriculum studi e accademico, Competenze professionali, Titolo di studio	Non sensibile
Contratti, Accordi,	Non sensibile
UTILIZZO DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO	
Finalità del Trattamento	Comunicazione e/o Trasmissione
Predisporre e redigere atti e/o contratti	
Tenuta delle scritture contabile	
Attività legate alla formazione	
	Commercialista
	Enti Pubblici e Privati

ELENCO DEI TRATTAMENTI DI DATI PERSONALI																		
Nominativo Incaricato	Mansione Funzione	Trattamenti																
		Raccolta	Registrazione	Organizzazione	Conservazione	Consultazione	Elaborazione	Modificazione	Selezione	Estrazione	Raffronto	Utilizzo	Interconnessione	Blocco	Comunicazione	Diffusione	Cancellazione	Distruzione
		si	si	si	si	si	si	si	si	si	si	si	si	si	si	si	si	si
		si	si	si	si	si	si	si	si	si	si	si	si	si	si	si	si	si

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	<input type="checkbox"/> Non esistente <input checked="" type="checkbox"/> Si, presente Tipo/Modello: Disco Rigido
Frequenza di backup:	<input type="checkbox"/> Giornaliera <input type="checkbox"/> Ogni due giorni <input checked="" type="checkbox"/> Settimanale
Incaricati del backup:	
Modalità Operative:	Al termine di ogni settimana lavorativa viene effettuato un backup completo su disco fisso di sicurezza
Supporti di backup:	Disco rigido di sicurezza
Etichettatura:	Sull'etichetta sono contenute le seguenti indicazioni: Data
Luogo di conservazione:	Ufficio n. Locali di Via P.S. Mattarella, n. 188, Via Quarto dei Mille, n. 20
Verifica backup:	La verifica del backup è effettuata confrontando le dimensioni dei file di backup con le dimensioni dei file originali.

SCHEDA RILEVAZIONE BANCHE DATI N. 02	
Codice:	BD02
Descrizione:	BANCA DATI FORNITORI. In questa banca dati sono conservati i dati dei fornitori del Consorzio.
Tipologia risorsa:	[x] Archivio Elettronico [X] Archivio Cartaceo
Ubicazione Banca Dati	Cartacea: Via P.S. Mattarella, n. 188, Via Quarto dei Mille, n. 20 Elettronica: Via P.S. Mattarella, n. 188, Via Quarto dei Mille, n. 20
Incaricati della Raccolta	
Risorse Hardware su cui è ospitata:	
NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO	
Dato	Natura del Dato
Nominativo, Indirizzo, Numero di telefono, telefax, etc	Non sensibile
Codice fiscale, Partita IVA,	Non sensibile
Assegni, Fatture, dati contabili	Non sensibile
Contratti, Accordi, transazioni, Identificativi finanziari	Non sensibile
UTILIZZO DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO	
Finalità del Trattamento	Comunicazione e/o Trasmissione
Predisporre e redigere atti e/o contratti	
Tenuta delle scritture contabile	
	Commercialista
	Enti Pubblici e Privati

ELENCO DEI TRATTAMENTI DI DATI PERSONALI																		
Nominativo Incaricato	Mansione Funzione	Trattamenti																
		Raccolta	Registrazione	Organizzazione	Conservazione	Consultazione	Elaborazione	Modificazione	Selezione	Estrazione	Raffronto	Utilizzo	Interconnessione	Blocco	Comunicazione	Diffusione	Cancellazione	Distruzione
		si	si	si	si	si	si	si	si	si	si	si	si	si	si	si	si	si
		si	si	si	si	si	si	si	si	si	si	si	si	si	si	si	si	si

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	<input type="checkbox"/> Non esistente <input checked="" type="checkbox"/> Si, presente Tipo/Modello: Disco Rigido
Frequenza di backup:	<input type="checkbox"/> Giornaliera <input type="checkbox"/> Ogni due giorni <input checked="" type="checkbox"/> Settimanale
Incaricati del backup:	
Modalità Operative:	Al termine di ogni settimana lavorativa viene effettuato un backup completo su disco fisso di sicurezza
Supporti di backup:	Disco rigido di sicurezza
Etichettatura:	Sull'etichetta sono contenute le seguenti indicazioni: Data
Luogo di conservazione:	Ufficio n. Via P.S. Mattarella, n. 188, Via Quarto dei Mille, n. 20
Verifica backup:	La verifica del backup è effettuata confrontando le dimensioni dei file di backup con le dimensioni dei file originali.

6. Elenco sedi ed uffici nei quali avviene il trattamento dei dati

Nella seguente tabella si elencano gli uffici dove si svolge il trattamento dei dati

Sede	Ufficio	Banca dati	Contenuto Banca Dati
Trapani (TP)	Via Pier Santi Mattarella, n. 188	BD01/BD02	Clienti/Fornitori
Palermo (PA)	Via Quarto dei Mille, n. 20	BD01/BD02	Clienti/Fornitori

7. Elenco cariche dei soggetti che effettuano il trattamento dei dati

Titolare del trattamento:

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

È onere del Titolare del trattamento, qualora lo ritenesse opportuno, individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati.

Il Titolare, a tal proposito, redigerà apposita lettera di incarico, nella quale elencherà in dettaglio le mansioni assegnate allo stesso.

Sarà cura del Titolare conservare in luogo sicuro una copia della lettera di incarico ed istruire adeguatamente i Responsabili in merito agli incarichi assegnati.

Il Titolare non può sottrarsi, anche se delega taluno, o al limite tutti gli aspetti gestionali ad altri soggetti, al compito di vigilare sul fatto che le norme privacy vengano diligentemente rispettate e che le misure di sicurezza vengano attuate.

Il Titolare del trattamento provvederà ad agevolare l'accesso ai dati personali da parte dell'interessato, a fornirgli le informazioni richieste e a ridurre i tempi per il riscontro del richiedente.

Nel caso di specie, Titolare del Trattamento è **UNISOM** nella persona del **Sig. Bertini Roberto** nato a Valderice (TP) il 06/09/1958, C.F.: **BRTRRT58P06G319T**, residente in Via Vespri, n. 257-91019 Valderice (TP).

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 20 di 34

Responsabile del trattamento:

La legge consente di nominare uno o più “responsabili del trattamento”, tali essendo la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. La nomina deve avvenire per atto scritto e deve contenere l'indicazione dei compiti assegnati a ciascun responsabile.

I Responsabili devono essere individuati fra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, con particolare riguardo alla sicurezza dei dati.

I Responsabili devono procedere al trattamento attenendosi alle istruzioni impartite dal titolare che, anche attraverso verifiche periodiche, deve vigilare sulla puntuale osservazione delle disposizioni di legge e delle istruzioni impartite.

Il Titolare del trattamento affida ai singoli Responsabili del trattamento l'onere di individuare, nominare ed indicare per iscritto uno o più Incaricati del trattamento.

I Responsabili del trattamento hanno il dovere di informare tempestivamente il Titolare di eventuali incidenti o della sopravvenuta mancanza dei requisiti minimi di sicurezza richiesti. A ciascun Responsabile del trattamento il Titolare del trattamento deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina dei Responsabili si intende a tempo indeterminato e decade o per dimissioni o per revoca comunicata per iscritto o con idonei mezzi informatici dal Titolare del trattamento.

La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

Per il trattamento dei dati personali il Titolare del trattamento **UNISOM** ha nominato i seguenti Responsabili, attribuendo loro incarichi di ordine organizzativo e direttivo, come segue:

- Responsabile per la sicurezza, il cui compito è di progettare, realizzare e mantenere in efficienza le misure di sicurezza, conformemente a quanto previsto dagli artt. 31 e 33 Dlgs 196/2003, nella persona della Sig.ra _____ nata a _____ il _____ e residente in _____ in Via _____, n. __, C.F.: _____;
- Responsabile del sistema informativo, cui è conferito il compito di sovrintendere alle risorse del sistema informativo e di consentirne l'utilizzazione, nella persona dell' _____, nato a _____ il _____, e residente in _____, in Via _____.
- Responsabile per garantire il soddisfacimento dei diritti esercitabili dai soggetti interessati, nella persona della Sig.ra Ambra Riggio nata a PALERMO il 14/01/1986 e residente in Palermo in Via Portello, n. 47-90135, C.F.: LNTLSN86A54G273C.

Incaricati del trattamento:

Nell' **UNISOM** il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico, mediante designazione per iscritto di ogni singolo incaricato, con il quale si individua puntualmente l'ambito del trattamento consentito.

Ogni incaricato deve attenersi alle istruzioni ricevute dal Titolare.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 21 di 34

- ▶ modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave
- ▶ prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
- ▶ procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
- ▶ procedure per il salvataggio dei dati
- ▶ modalità di custodia ed utilizzo dei supporti rimovibili, contenenti dati personali
- ▶ dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

La nomina degli Incaricati del trattamento viene controfirmata dall'interessato per presa visione e copia della stessa viene conservata a cura del Titolare del trattamento per la sicurezza dei dati in luogo sicuro.

Compito degli Incaricati è quello di svolgere gli incarichi assegnati, dettagliatamente specificati nella lettera di incarico, sempre nel pieno rispetto del presente DPSS. In caso di incidenti o di conoscenza di circostanze che possano far venire meno i requisiti minimi di sicurezza, gli Incaricati dovranno comunicare tempestivamente tale circostanza al Titolare del trattamento o, in mancanza, al Titolare.

La nomina degli Incaricati è a tempo indeterminato, e decade per revoca, per sue dimissioni, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

Il Consorzio **UNISOM** ha nominato i seguenti Incaricati del trattamento:

N°	Nominativo	Luogo di nascita	Data di Nascita	Codice Fiscale	Mansione
1	AMBRA RIGGIO	Palermo	15/06/1985	RGGMBR85H55G273M	Segreteria Amministrativa
2					

Custode delle credenziali di autenticazione:

Il Responsabile, di concerto con il Titolare, ha nominato un custode delle credenziali di autenticazione per l'accesso ai sistemi di elaborazione dati. L'incarico è stato assegnato per iscritto e la lettera controfirmata dall'interessato per presa visione è conservata in un luogo sicuro da parte del soggetto che conferisce l'incarico.

E' compito del Custode delle credenziali predisporre, per ogni incaricato del trattamento, una busta sulla quale è indicato il nominativo dell'Incaricato, all'interno della busta, su apposito modulo, vengono indicate lo User-Id utilizzato e le relative password d'accesso.

Il Custode delle credenziali deve revocare tutte le password non utilizzate per un periodo superiore a 6 (sei) mesi.

La nomina del Custode delle credenziali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del Custode delle credenziali può essere revocata in qualsiasi momento senza preavviso, ed essere affidata ad altro soggetto.

- Nel consorzio **UNISOM** è stato designato quale Custode il **Sig. Bertini Roberto** nato a Valderice (TP) il 06/09/1958, C.F.: **BRTRRT58P06G319T**. Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro dei compiti di ciascuno nell'ambito del trattamento dei dati personali.

Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

8. Analisi dei Rischi

In data odierna è stata aggiornata l'analisi dei rischi in relazione alle risorse coinvolte, a vario titolo, tenendo conto, altresì, del progresso tecnologico, della sostituzione, integrazione e acquisizione di nuovo hardware, degli aggiornamenti o della sostituzione dei Sistemi Operativi e/o dei programmi applicativi.

Per Analisi dei Rischi si intende lo studio delle minacce e delle vulnerabilità a cui sono soggette le risorse. Gli indici di rischio sono fissati mediante una scala articolata a 3 valori come di seguito riportati nel presente documento.

L'Analisi è stata eseguita in maniera distinta sulle categorie di beni individuati precedentemente.

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 23 di 34

8.1. Analisi dei Rischi sulle Aree e sui Locali

Risorsa	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
Tutte	Accesso nei locali dove si svolge il trattamento (rapine, furti, atti vandalici)	Bassa	L'accesso agli uffici è sempre controllato durante il normale svolgimento dell'attività lavorativa.
Tutte	Allagamenti	Bassa	Area non soggetta ad inondazioni o calamità di questo tipo.
Tutte	Incendio	Bassa	La sede è provvista di dispositivi antincendio.
Tutte	Corto circuito	Bassa	Impianto a norma CEE provvisto di gruppo di continuità

8.2. Analisi dei Rischi sulle Risorse Hardware

Risorsa	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
Tutte	Uso non autorizzato dell'hardware	Bassa	L'utilizzo dell'hardware è soggetto all'utilizzo di credenziali d'accesso.
Tutte	Manomissione/Sabotaggio	Bassa	Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da tecnici autorizzati.
Tutte	Probabilità/Frequenza di guasto	Bassa	L'hardware acquistato è di qualità.
Tutte	Rischi connessi all'elettricità	Bassa	Gli elaboratori sono dotati di gruppo di continuità che fornisce energia di buona qualità (stabilizzazione) e impedisce l'improvvisa assenza di corrente elettrica.

8.3. Analisi dei Rischi sulle Risorse Software

Risorsa	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
Sistema Operativo	Danneggiamento fisico dei dati in fase di copia o di spostamento da un'unità ad un'altra	Bassa	Vengono effettuate copie settimanali di backup delle banche dati.
Sistema Operativo	Blocco del Sistema Operativo con relativa perdita di dati in memoria o scrittura di informazioni errate o incomplete nella Banca Dati.	Bassa	Vengono effettuate copie settimanali di backup delle banche dati.
Sistema Operativo	Errato uso del Sistema Operativo	Bassa	Vengono effettuate copie settimanali di backup

			delle banche dati.
Sistema Operativo	Intrusione da parte di soggetti estranei o non autorizzati al trattamento dei dati	Bassa	Le risorse sono protette da un idoneo "firewall" software.
Applicativo	Errori software che minacciano l'integrità dei dati	Bassa	I software sono utilizzati da parecchi anni e non hanno mai causato la perdita o il danneggiamento dei dati trattati. I software vengono aggiornati con cadenza almeno semestrale.
Applicativo	Danneggiamento in sede di trattamento dei dati	Bassa	Vengono effettuate copie settimanali di backup delle banche dati.
Applicativo	Errata installazione o errato uso del software	Bassa	Vengono effettuate copie settimanali di backup delle banche dati.
Applicativo	Accesso consentito ad utenti non autorizzati	Bassa	Vengono periodicamente verificate le credenziali di accesso
Applicativo	Errato uso dell'applicativo	Bassa	Vengono effettuate copie giornaliere di backup delle banche dati.
Tutte	Presenza di codice non conforme alle specifiche del programma	Bassa	I programmi sono forniti da produttori che operano nel settore con la massima serietà da molti anni.

8.4. Analisi dei Rischi sulle Banche Dati

Banca Dati	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
Tutte	Accesso non autorizzato	Bassa	L'accesso alle risorse dati in formato elettronico avviene solo tramite gli elaboratori protetti dall'utilizzo di credenziali d'accesso. All'archivio cartaceo possono accedere solo i diretti incaricati dopo aver richiesto le chiavi del locale al responsabile.
Tutte	Intrusione da parte di soggetti	Bassa	Le risorse sono protette

	estranei o non autorizzati al trattamento dei dati		con idoneo firewall software.
Tutte	Perdita di dati	Bassa	Vengono effettuate copie settimanali di backup delle banche dati. I PC sono dotati di Software Antivirus costantemente aggiornato.
Tutte	Incapacità di ripristinare copie di backup	Bassa	I controlli periodici effettuati sui supporti di backup hanno sempre fornito esiti positivi.

Legenda: Soglie di Rischio

Soglia	Descrizione
Bassa	Con questa soglia viene individuato un rischio molto basso che identifica una minaccia remota e comunque rapidamente reversibile od ovviabile.
Media	Con questa soglia viene individuato un rischio superiore al precedente identificante una minaccia remota ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tale caso è già consigliabile pensare ad accorgimenti per contenere il rischio.
Grave o Gravissimo	Li trattiamo insieme perché con queste soglie vengono individuati rischi che è sicuramente inaccettabile pensare di correre. Pertanto dovrà sicuramente essere attivato un insieme di contromisure (di natura fisica, logica, etc..) per abbattere il rischio e contenerlo in livelli accettabili.

9. Definizione ed Attuazione della Politica di Sicurezza

Al fine di assicurare l'integrità dei dati trattati ed impedirne la comunicazione e/o diffusione non autorizzata, il consorzio **UNISOM** ha elaborato una precisa Politica di Sicurezza basata sull'adozione di misure di tipo **fisico, logico** ed **organizzativo**. Tali misure avranno il compito di garantire sia i minimi requisiti di sicurezza contemplati dal Disciplinare Tecnico (allegato B del D.L.vo 196/2003), sia un livello idoneo di sicurezza relativamente alle tipologie dei nostri dati trattati, alle modalità di trattamento ed agli strumenti utilizzati.

9.1. Misure di Sicurezza di tipo Fisico adottate

Descrizione Misura	Criteri per la corretta applicazione
Custodia degli archivi cartacei in armadi chiusi a chiave.	Tutti i documenti cartacei contenenti dati personali sono conservati nei locali archivio in armadi dotati di serratura. Gli incaricati possono prelevare i documenti necessari per il trattamento per il tempo necessario a tale operazione dopo di che avranno il compito di riporli nel sopracitato luogo preposto alla loro conservazione. Sarà compito dell'incaricato che preleva i documenti garantire che questi ultimi siano rinchiusi, sotto chiave, in un cassetto della propria scrivania nel periodo di temporanea assenza dal posto di lavoro.
Custodia dei supporti	I supporti che vengono utilizzati per l'attività di backup sono conservati in un armadio interno al locale di archivio.
Continuità dell'alimentazione elettrica	Gli elaboratori sono collegati a gruppi di continuità che garantiscono una stabilizzazione dell'energia elettrica erogata. Questi gruppi, in conseguenza di un'improvvisa assenza di energia, garantiscono un'autonomia temporale necessaria ad avviare le corrette procedure di spegnimento degli elaboratori.
Verifica della leggibilità dei supporti di backup	Sistematicamente dopo aver fatto la copia di backup settimanale, l'incaricato ne testa il contenuto dei dati registrati verificando nel contesto l'integrità.
Dispositivi antincendio	I locali della sede sono dotati di estintori per la soppressione di eventuali focolai di incendio.

9.2. Misure di Sicurezza di tipo Logico adottate

Descrizione Misura	Criteri per la corretta applicazione
<p>Realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato</p>	<p>Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare.</p> <p>E' impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico.</p> <p>Per realizzare le credenziali di autenticazione si utilizza il seguente metodo:</p> <ul style="list-style-type: none"> ▶ si associa un codice per l'identificazione dell'incaricato (<i>username</i>), attribuito da chi amministra il sistema, ad una parola chiave riservata (<i>password</i>), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente <p>Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:</p> <ul style="list-style-type: none"> ▶ ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale. ▶ la credenziale di autenticazione costituita dal codice per l'identificazione (<i>username</i>), attribuito all'incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi. <p>Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:</p> <ul style="list-style-type: none"> ▶ immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento ▶ in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.
<p>Assegnazione ed autorizzazione degli elaboratori su cui effettuare i trattamenti</p>	<p>Ogni incaricato può beneficiare dell'accesso su un elaboratore tramite il quale potrà entrare negli archivi in formato elettronico su cui operare i trattamenti.</p>
<p>Indicazione del custode delle credenziali (o preposto)</p>	<p>E' stato individuato e nominato per iscritto il custode delle credenziali a cui spetta la custodia, in un luogo sicuro, delle password a lui affidate dagli incaricati.</p>

Indicazione sui requisiti minimi, che gli incaricati devono utilizzare nell'elaborare e modificare la <i>parola chiave (password)</i> , che permette loro di accedere agli strumenti	<p>Elaborare la <i>password</i>, e conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (<i>username</i>).</p> <p>La password deve essere composta da almeno otto caratteri. E' buona norma che, di questi caratteri, da un quarto alla metà siano di natura <i>numerica</i>.</p> <p>La password non deve contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici)</p> <p>L'incaricato deve <i>provvedere a modificare la password</i>, con la seguente tempistica:</p> <ul style="list-style-type: none"> ▶ <i>immediatamente</i>, non appena la riceve per la prima volta, da chi amministra il sistema; ▶ successivamente, <i>almeno</i> ogni sei mesi. Il termine scende a tre mesi, se la parola chiave dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari; ▶ le password comunicate ai fini dell'assistenza sistemistica agli incaricati, vanno sostituite al termine dell'intervento.
Autorizzazione al personale esterno addetto alla manutenzione	E' stato autorizzato per iscritto il personale esterno addetto alla manutenzione dei componenti hardware e software.
Predisposizione ed aggiornamento degli Antivirus	Gli elaboratori sono protetti con idonei programmi Antivirus. Le "firme" dei virus vengono aggiornate con cadenza quindicinale.
Predisposizione idonei strumenti di protezione perimetrale	Gli elaboratori contenenti dati sensibili sono protetti con idoneo firewall software.

9.3. Misure di Sicurezza di tipo Organizzativo adottate

Descrizione Misura	Note ed indicazioni per la corretta applicazione
Analisi dei Rischi e Documento Programmatico Sulla Sicurezza	Sulla base dell'analisi dei rischi è stato redatto il presente documento programmatico sulla sicurezza. Questo documento sarà divulgato a tutte le funzioni dell' UNISOM
Prescrizione di linee-guida di sicurezza	Sono state redatte le linee-guida sul corretto utilizzo del sistema informativo. Questo documento sarà divulgato a tutte le funzioni dell' UNISOM
Piano di verifica delle misure adottate	E' stato stabilito un piano di verifica delle misure adottate. Tale piano è illustrato nel presente DPSS al capitolo 12.
Piano di formazione degli incaricati	E' stato predisposto un piano di formazione degli incaricati. Tale piano è illustrato nel presente DPSS al capitolo 13.
Custodia di documenti cartacei	Tutti i documenti cartacei contenenti dati personali, tranne per i periodi strettamente necessari alle operazioni di trattamento, sono custoditi in armadi blindati dotati di serratura all'interno del locale archivio.

9.4. Misure adottate per garantire l'integrità e la disponibilità dei dati

In esecuzione del punto 19.4 dell'allegato B al D.Lgs 196/2003, al fine di garantire l'integrità e la disponibilità dei dati, la protezione delle aree e dei locali, si descrivono le seguenti misure di sicurezza già adottate dal Consorzio, nel momento in cui viene redatto il presente documento:

La protezione delle aree e dei locali

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si svolge il trattamento non sono protetti da sistemi di allarme.

Le aree contenenti dati in supporto cartaceo (archivio e mobili contenenti documentazione) sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso.

L'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Gli impianti ed i sistemi di cui è dotata l'organizzazione appaiono appena sufficienti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti. Per l'anno 2011 sono previsti degli interventi atti a migliorare ed ottimizzare quanto in dotazione come ad esempio estintori e gruppi di continuità.

L'archiviazione e custodia di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, devono rivolgersi direttamente al titolare.

Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali.

Gli impianti e le attrezzature, per la custodia e l'archiviazione di atti, documenti e supporti:

- ▶ appaiono soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti. Per l'anno 2011, sono quindi previsti semplicemente interventi di manutenzione e di rimpiazzo

10. Criteri e modalità di ripristino dei dati

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli.

I documenti cartacei, e gli eventuali supporti diversi da quelli elettronici, contenenti dati personali, vengono fotocopiati, con cadenza mensile.

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 30 di 34

I supporti contenenti le copie vengono archiviati in appositi armadi.

Gli investimenti programmati per il 2011, finalizzati a garantire il ripristino dei dati in termini ragionevoli, sono investimenti in strumenti di backup.

11. L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- ▶ dal Dlgs 196/2003, se il terzo destinatario è italiano
- ▶ dalla direttiva 95/46/CE, se il terzo destinatario non è italiano.

Qualora il trasferimento avvenga verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 Dlgs 196/2003, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **sensibili o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano:

- ▶ rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.

Allo stato attuale, risultano nominati come responsabili:

- ▶ Consulenza contabile: Studio Montemario con studio in Via Colonnello Romei, 15-91100 -Trapani ;
- ▶ Consulenza del lavoro: Studio Stella Grammatico con sede in Via G.B. Fardella, 13091100 -Trapani,

Allegato 01	<i>UNISOM</i>	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 31 di 34

12. Piano di Verifica delle Misure adottate

Al responsabile per la sicurezza è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile per la sicurezza e le persone da questo appositamente incaricate provvedono con frequenza mensile, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- ▶ verificare l'accesso fisico ai locali dove si svolge il trattamento
- ▶ verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- ▶ monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette
- ▶ verificare l'integrità dei dati e delle loro copie di backup
- ▶ verificare la sicurezza delle trasmissioni in rete
- ▶ verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
- ▶ verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

Dell'attività di verifica svolta viene redatto un verbale, che viene conservato dal Titolare.

13. Piano di Formazione degli Incaricati

Il Titolare ha provveduto all'opportuna formazione di tutti gli incaricati al trattamento dei dati al fine di:

1. garantire il massimo rispetto delle procedure elencate nel presente DPSS;
2. rendere edotto il personale sui rischi che incombono sui dati e le modalità su come prevenire i danni (Disciplinare Tecnico del T.U);
3. informare il personale sulle responsabilità che ne derivano.

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

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

Allegato 01	<i>UNISOM</i>	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 32 di 34

Nello schema che segue, sono elencate le basilari necessità di formazione dei soggetti nominati quali Incaricati del trattamento.

Formazione da impartire	Intervento formativo
Custodia dello strumento elettronico durante una sessione di trattamento di dati personali	Con apposito corso formativo, organizzato a cura del Responsabile del Trattamento, è necessario sensibilizzare il personale incaricato al trattamento e alla custodia dello strumento elettronico in particolare durante una sessione di trattamento.
Rischi incombenti sui dati	Apposito corso formativo atto ad illustrare i rischi incombenti sui dati
Misure preventive di eventi dannosi	Sensibilizzazione del personale incaricato del trattamento a non attuare azioni che possano danneggiare gli elaboratori elettronici ed i dati in essi contenuti. Il personale incaricato deve essere ammonito sulle responsabilità, a loro carico, dettate dalla normativa vigente e deve essere sensibilizzato sulle misure minime di sicurezza da adottare.
Conoscenza delle norme e del DPSS o delle parti rilevanti in relazione al trattamento dei dati ed al settore di attività aziendale	Attenta lettura dell'allegato B del D.Lgs 196/2003 e del Documento di Programmazione sulla Sicurezza dei dati Personali. Si deve rapportare la norma alle esigenze della nostra attività aziendale chiarendo, contestualmente, i dubbi che il personale incaricato del trattamento ha posto. Inoltre, bisogna fornire a tutti i soggetti elencati una copia del D.Lgs 196/2003 ed una copia del DPSS.
Custodia ed uso dei supporti rimovibili contenenti dati personali, sensibili o giudiziari.	Il responsabile del trattamento deve fornire apposite istruzioni descritte e dettagliate. Quindi, necessita invitare il personale incaricato del trattamento a non lasciare incustoditi i supporti rimovibili contenenti dati personali, a non condurre supporti rimovibili all'esterno degli uffici in cui il trattamento è effettuato. Infine, è fatto assoluto divieto di condurre dati sensibili o giudiziari all'esterno dei locali in cui si effettua il trattamento se non preventivamente autorizzati e con l'osservanza della procedura illustrata

Controllo e custodia per l'intero ciclo di trattamento di dati senza supporto di strumenti elettronici	Le procedure per il controllo, la custodia ed il trattamento di dati personali senza l'ausilio di strumenti elettronici sono descritti nell'apposita procedura. A cura del responsabile deve essere organizzato apposito corso formativo che dovrebbe coinvolgere tutti gli incaricati elencati ed in cui dovrà essere illustrato il documento sopramenzionato e dove verranno chiariti ulteriori quesiti posti dagli incaricati.
--	---

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale.

Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali.

Inoltre, essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare se un dato possa avere o meno natura sensibile o giudiziaria.

La formazione è fatta dal Titolare del Trattamento.

Coerentemente con l'evoluzione degli strumenti tecnici adottati dal **CONSORZIO UNIVERSITARIO PER L'ATENEO DELLA SICILIA OCCIDENTALE E DEL BACINO DEL MEDITERRANEO** e/o dall'insorgere di nuove disposizioni legislative in materia, verranno istituiti nuovi incontri formativi. In ogni caso, almeno una volta l'anno, verrà comunque istituito un incontro per risensibilizzare gli incaricati sull'importanza di adottare le norme di sicurezza predisposte e per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

14. Dichiarazioni d'impegno e firma

Il presente documento, redatto nel Marzo 2011, viene firmato in calce dal Sig. Bertini Roberto, in qualità di Responsabile Legale.

L'originale del presente documento viene custodito presso la sede del Consorzio, per essere esibito in caso di controlli.

TRAPANI (TP), _____

Firma del Titolare del Trattamento

Allegato 01	UNISOM	Rev. n. 03 del 31.03.2011
Documento Programmatico sulla Sicurezza dei Dati		Pagina 34 di 34