Consorzio di Bonifica del Sannio Alifano
Piedimonte Matese (Caserta)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

di cui al Decreto Legislativo 30 giugno 2003 n. 196, approvato con deliberazione commissariale n° 58/06 del 30/03/2006

1. Scopo del Documento

Scopo del presente documento è stabilire le misure di sicurezza, organizzative, fisiche e logiche, da adottare presso il Consorzio di Bonifica del Sannio Alifano affinché siano rispettati gli obblighi previsti dal Codice in materia di protezione dei dati personali, D. Lgs. 30 giugno 2003, n. 196, e dal Disciplinare tecnico relativo alle misure minime di sicurezza obbligatorie per il trattamento dei dati personali.

2. Definizioni

- *dato personale*: qualunque informazione relativa a persona fisica, persona giuridica, ente od 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.
- *dati sensibili*: dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
- *dati giudiziari*: dati personali idonei a rivelare la posizione giudiziaria di un interessato.
- *misure minime di sicurezza*: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza volte a minimizzare 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.
- *archivi*: gli archivi che contengono i dati e le informazioni oggetto di trattamento possono essere informatici (dischi fissi e rimovibili di personal computer, compact disk, nastri magnetici, e altri minori) oppure cartacei (tutti i supporti, diversi da quelli informatici, che contengono in qualunque forma dati o informazioni personali incluse le copie su carta di dati gestiti con supporti informatici).
- *gateway*: è definito "gateway" per le interconnessioni esterne l'insieme di hardware, software e applicazioni che permettono l'interconnessione o l'accesso remoto.

3. Elenco dei trattamenti

L'analisi compiuta sull'attività svolta dal Consorzio ha permesso di individuare le seguenti tipologie di trattamenti:

Funzione	Trattamento	Categorie di Interessati	Tipologia dei dati	Tipologia archivio
Amministrazione e Finanza	Gestione della contabilità banche Gestione della riscossione Gestione della contabilità fornitori	Banche, Soggetti terzi, Consorziati, Consulenti, Fornitori	Anagrafici Contabili Finanziari	Informatico Cartaceo
Affari Generali	Gestione Contrattualistica Gestione Gare Supporto agli organi consortili	Fornitori, Consulenti, Soggetti terzi, Organi consortili	Anagrafici Contabili Finanziari Giudiziari	Cartaceo
Catasto	Acquisizione dati Aggiornamento dati Gestione volture Servizio informativo	Consorziati Enti Pubblici	Anagrafici Anagrafici immobiliari	Informatico Cartaceo
Espropri	Acquisizione dati	Consorziati Enti Pubblici	Anagrafici Anagrafici immobiliari Finanziari Giudiziari	Informatico Cartaceo
Personale	Selezione e formazione del personale Trattamento Economico Adempimenti contabili Adempimenti fiscali e contributivi Visite mediche	Dipendenti Enti Pubblici Sindacati	Anagrafici Anagrafici sensibili Anagrafici giudiziari	Informatico Cartaceo

Il trattamento dei dati avviene nella sede del Consorzio situata in Viale della Libertà – 81016 Piedimonte Matese (CE).

Gli *uffici*, dislocati su tre livelli, sono organizzati come segue:

a) piano rialzato - area tecnico-agraria settore catasto: l'accesso al pubblico è consentito negli orari prestabiliti (dal lunedì al venerdì dalle 9.00 alle 13.00).

b) primo piano – area amministrazione e finanza, settore affari generali, settore personale e settore ragioneria: l'accesso è consentito solo al personale dipendente del Consorzio e alle persone autorizzate.

c) secondo piano – area tecnico agraria settore espropri, opere idrauliche e opere irrigue: l'accesso è consentito solo al personale dipendente del Consorzio e alle persone autorizzate.

E' in fase di realizzazione una portineria d'accesso agli uffici.

Gli *archivi* hanno una collocazione distribuita sui tre piani e di seguito distinta:

- Archivio piano rialzato: contiene dati, informazioni e documenti di competenza dell'area tecnico-agraria settore catasto ed è dotato di porta d'accesso con chiusura a scatto. Pur essendo presenti documenti su supporti cartacei, tutti i dati oggetto di trattamento sono archiviati su supporti informatici. L'accesso, sorvegliato negli orari di apertura al pubblico, è consentito ai soli incaricati dal Responsabile del trattamento.
- Archivio primo piano: è separato in due locali distinti che contengono dati, informazioni e documenti rispettivamente di competenza dei settori affari generali e personale e del settore ragioneria ed è dotato di porta d'accesso con chiusura a scatto. L'archivio contiene dati sia su supporti cartacei che informatici. L'accesso è consentito ai soli incaricati dal Responsabile del trattamento.
- Archivio secondo piano: contiene dati, informazioni e documenti di competenza dell'area tecnico-agraria settore espropri, opere idrauliche e opere irrigue ed è dotato di porta d'accesso con chiusura a scatto. L'archivio contiene dati sia su supporti cartacei che informatici. L'accesso è consentito ai soli incaricati dal Responsabile del trattamento.

4. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.

I termini Titolare del trattamento, Responsabile del trattamento, Incaricato del trattamento, Custode delle password e Dati personali sono usati in conformità alle definizioni dettate dal Codice in materia di protezione dei dati personali.

Al *Titolare* competono le decisioni in ordine alle finalità e alle modalità del trattamento di dati personali.

Per il trattamento dei dati personali il Titolare ha nominato il dott. Fabrizio Pepe quale Responsabile preposto al trattamento e alla sicurezza dei dati. La nomina è avvenuta in data ……. con delibera ……..(allegato A).

Il Titolare ha il compito di vigilare, anche tramite verifiche periodiche, sul rispetto, da parte del Responsabile, delle proprie istruzioni, nonché sulla

osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Il Titolare, inoltre, garantisce, al Responsabile di trattamento, il supporto in termini di adeguati budget e deleghe di autorità, affinché possa svolgere in autonomia e responsabilità i compiti affidati.

Il *Responsabile* dei trattamenti e della sicurezza dei dati personali ha la responsabilità di:

- promuovere lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel Documento Programmatico sulla Sicurezza dei dati personali;
- informare il Titolare del trattamento sulle non conformità con le norme di sicurezza e su eventuali incidenti;
- garantire lo svolgimento di un continuo processo di addestramento degli Incaricati del trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza;
- assicurare che vengano effettuati test periodici per verificare l'efficacia delle contromisure di sicurezza adottate;
- valutare almeno annualmente il livello di rischio cui sono esposti i dati personali oggetto di trattamento e aggiornare il relativo documento.

Nell'ambito della struttura del Consorzio, il dott. Fabrizio Pepe riveste anche il ruolo di Responsabile dei c.d. "trattamenti informatici". Tale inquadramento implica le responsabilità tipiche dei trattamenti informatici e di seguito indicate:

- gestione tecnica dei sistemi;
- gestione dei Log. di accesso;
- gestione tecnica e organizzazione degli archivi informatici;
- gestione delle copie di backup;
- custodia delle applicazioni, delle banche dati e della rete;
- definizione delle procedure di gestione delle user ID (normali e con autorità – la distinzione può rendersi necessaria in base al tipo di dati visibili e gestibili in rete) e delle password;
- garantire l'aggiornamento del presente DPS secondo l'evoluzione tecnologica;
- assicurare controlli e verifiche tecniche, secondo periodicità stabilite, in merito al rispetto delle prescrizioni contenute nel presente DPS, e più in generale nel Codice privacy;

- definire e promuovere sessioni periodiche di addestramento e di aggiornamento sulla sicurezza per gli incaricati.

Sarà facoltà del Responsabile preposto ai trattamenti informatici nominare:

- un *amministratore di sistema* che sovrintenda alle risorse dei sistemi operativi dei computer, dei sistemi della base dati e ne consenta l'uso; fornisca guida e supporto agli incaricati; amministri e gestisca, dal punto di vista tecnico, la sicurezza informatica dei sistemi a lui assegnati; sviluppi, realizzi e aggiorni le misure di sicurezza, per le banche dati personali, in accordo con le norme del DPS;
- un *custode delle password* nella qualità di incaricato del trattamento al quale venga assegnato il compito di custodire le password per l'accesso ai dati; amministrare gli strumenti tecnici che gestiscono e proteggono le parole chiave; garantire la segretezza delle credenziali di autenticazione; assicurare la disponibilità di dati e strumenti elettronici nel caso in cui l'assenza prolungata o l'impedimento dell'Incaricato renda indispensabile un accesso allo strumento informatico da lui utilizzato.

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto. L'incarico non è disposto a titolo individuale, ma consegue in modo diretto dalla documentata assegnazione del dipendente ad una area per la quale è individuato per iscritto l'ambito di trattamento consentito, vale a dire l'insieme delle operazioni di trattamento autorizzate e le regole ad esse applicabili.

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli *Incaricati* sono fornite esplicite istruzioni relativamente a:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere ai sistemi elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola 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 di salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimuovibili contenenti dati personali;
- aggiornamento continuo, utilizzando le fonti fornite dal Responsabile del trattamento, sulle misure di sicurezza da adottare.

Agli Incaricati al trattamento, il Responsabile fornisce la necessaria formazione:

- al momento dell'ingresso in servizio;
- in occasione dei cambiamenti di mansione;
- in occasione dell'introduzione di nuovi strumenti e programmi informatici.

Gli Incaricati del trattamento dei dati personali, nell'ambito del trattamento assegnato, hanno le seguenti responsabilità:

- svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel Documento Programmatico sulla Sicurezza e le direttive del Responsabile;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile del trattamento;
- rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il Responsabile del trattamento in caso di incidente di sicurezza che coinvolga dati personali.

5. Analisi dei rischi

L'analisi dei rischi, tenuto conto della tipologia dei dati trattati e delle caratteristiche degli strumenti utilizzati per il trattamento dei dati, è stata focalizzata sulle circostanze, possibili o probabili, che possono determinare la distruzione o la perdita, anche accidentale, dei dati, l'accesso non autorizzato, il trattamento non consentito o non conforme alle finalità della raccolta.

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

- *intergità dei dati*: intesa come la gestione dell'accuratezza e completezza delle informazioni e delle relative applicazioni, la salvaguardia dell'esattezza dei dati, la difesa da manomissioni o modifiche non autorizzate, ecc.;
- *riservatezza*: intesa come la garanzia che le informazioni siano accessibili solo alle persone autorizzate, la protezione delle trasmissioni, il controllo degli accessi, ecc.;

- *disponibilità dei dati*: intesa come l'assicurazione che l'accesso ai dati sia disponibile quando necessario, quindi la garanzia per gli utenti della fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi stessi.

Poiché le informazioni siano soggette a un rischio occorre che una minaccia sfrutti una o più debolezze presenti nel sistema di sicurezza.

Il metodo utilizzato non si sofferma ad analizzare in dettaglio tutte le diverse tipologie di minacce possibili, ma le sintetizza raggruppandole per grandi famiglie. La sempre maggiore diffusione di reti informatiche condivise e l'utilizzo generalizzato di internet tende oggi a rendere omogenee, per settori di attività, le minacce e la probabilità che si concretizzino.

L'analisi dei rischi prende in esame l'intera struttura dell'Ente ed è stata suddivisa nelle seguenti aree:

- politica della sicurezza: il sistema di sicurezza si deve basare su taluni principi fondamentali che l'Ente rende propri come valori irrinunciabili. Scopo primario è quello di diffondere la consapevolezza sui rischi che corrono le informazioni personali e definire le responsabilità in materia.
- organizzazione della sicurezza: qualsiasi sistema di sicurezza adeguato si fonda su una corretta distribuzione di ruoli e responsabilità. Una organizzazione della sicurezza è efficace se gode del supporto degli organi direttivi e di adeguati budget. Occorre, inoltre, evitare i conflitti di interesse nell'ambito della struttura organizzativa che si è predisposta.
- classificazione e controllo: la sicurezza delle informazioni presuppone la conoscenza, la gestione e il controllo delle stesse. I dati personali comuni, quelli sensibili e gli altri dati trattati dall'Ente vanno classificati per poterli distinguere e proteggere in modo selettivo.
- condotta del personale: le rilevazioni statistiche delle casistiche degli accessi non autorizzati ai sistemi informatici indicano che le effrazioni sono prevalentemente di origine interna. Per migliorare l'efficacia dei sistemi di protezione è fondamentale poter contare su adeguati e consapevoli comportamenti di tutto il personale.
- sicurezza fisica e ambientale: le apparecchiature critiche e gli archivi dovrebbero essere sempre posti in ambienti sicuri, con accesso controllato e dotati di sistemi di protezione ambientali. La gestione degli accessi, sia del personale interno sia di quello di terzi, dovrebbe essere sempre regolato da rigorose procedure.

- gestione dei computer e della rete: gli ambienti intranet e internet sono sempre più complessi e richiedono molta attenzione, così come ogni altro tipo di connessione con l'esterno (linee telefoniche, modem) nonché la crescente minaccia di virus e di altri programmi "pericolosi". Nel caso di outsourcing di servizi di vario genere è necessario predisporre chiari contratti in materia di sicurezza.
- procedure di accesso ai sistemi e ai dati: non basta usare user-ID e password, ma occorre che le autorizzazioni siano date a ragion veduta e soprattutto ritirate quando non più necessarie. Una gestione non rigorosa di tali elementi è segnale di basso livello di sicurezza. E' essenziale, inoltre, che i log di accesso siano registrati e regolarmente controllati. Gli utenti devono avere la consapevolezza che gli accessi e i tentativi di accesso sono rilevati.
- piano di continuità: il piano di continuità dovrebbe comprendere il deposito dei dati di backup degli archivi e degli ambienti applicativi, in locali separati da quelli dei dati originari e l'effettuazione di test periodici per verificarne l'efficacia e lo stato di aggiornamento.
- archivi cartacei: la sicurezza degli archivi cartacei, oltre che con opportune apparecchiature, si raggiunge con una intensa azione di formazione ed addestramento. Anche i migliori armadi corazzati risultano inutili se gli incaricati del trattamento lasciano l'ufficio incustodito senza adottare le necessarie misure di sicurezza.
- gestione workstation: dal punto di vista della sicurezza le workstation rappresentano una debolezza di non facile contenimento. Non sempre il sistema operativo utilizzato dispone di adeguate misure di sicurezza ed a volte è facilmente modificabile dall'utente. Inoltre è sempre possibile riprodurre e registrare sulle workstation copie, anche voluminose, di porzioni di banche dati con scarsa possibilità di controlli.
- servizi in outsourcing: con il termine "outsourcing" si intende l'affidamento a terzi di servizi per conto dell'Ente. La legge prevede che, qualora tali servizi prevedano trattamento di dati personali, i fornitori del servizio siano inquadrati in specifici ruoli da cui discendono diverse forme di responsabilità. Eventuali carenze in questa area possono avere ripercussioni legali e di immagine per l'Ente.

Dalle interviste effettuate con le persone di riferimento per i vari trattamenti, risulta che la tipologia delle minacce più sentite sono oltre le esterne quelle interne. Ciò per la consapevolezza di una non diffusa formazione del personale in tema di sicurezza e da un non sistematico controllo che le norme tecniche-

organizzative emesse in materia di sicurezza delle informazioni siano rispettate dagli outsoucer.

Di seguito i dettagli della rilevazione sulla percezione delle minacce:

%	Probabilità	rating
minore del 10%	scarsa / bassa	1
compreso tra 11% e 50%	possibile / medio – bassa	2
compreso tra 51% e 90%	probabile / media	3
Oltre il 90%	certa / alta	4

Il "rating probabilità" indica la probabilità (in termini qualitativi) che l'evento si avveri.

Tipologia di minaccia			Danno	Rating probabilità
Casuali	Malfunzionamenti	Hardware	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Software	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Rete	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
	Eventi naturali	Terremoto	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Inondazioni	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Frane	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Folgorazioni	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Eventi meteo (vento, grandine, neve)	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
	Fenomeni ambientali	Elettricità (incendio, caduta di tensione, ecc.)	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Allagamento (impianto di condizionamento, servizi igienici, ecc.)	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
Non Casuali	Programmi SW pericolosi	Virus	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Applicazioni errate o non compatibili	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
	Esplosioni		☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
	Interferenze e intrusioni	Rete	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
	Malfunzionamenti	Interconnessioni o	☐ riservatezza	☐ 1 ☐ 2 ☐ 3 ☐ 4

		accesso remoto	☐ integrità ☐ disponibilità	
Interne	Personale	Addetti ai computer	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Utenti autorizzati	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Consulenti	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
Esterne	Corrieri		☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
	Manutenzione	Tecnici di manutenzione hardware e software	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Tecnici degli impianti	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
		Addetti alle pulizie	☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
	Hacker		☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4
	Elementi criminali		☐ riservatezza ☐ integrità ☐ disponibilità	☐ 1 ☐ 2 ☐ 3 ☐ 4

Gli indici di rischio sono riferiti ai 3 valori sotto riportati:

Indici di rischio	**Descrizione**
BASSO	Situazione in linea con gli standard di sicurezza più diffusi. L'Ente dimostra diligenza nell'applicazione delle contromisure e sono rispettate le prescrizioni di legge. E' sufficiente una normale attività di manutenzione per mantenere la situazione ad un adeguato livello di efficienza.
MEDIO	Situazione con deficienze note. Il livello di protezione è discontinuo e poco omogeneo. Se non si interviene in tempi certi il rischio passa a livello alto. Per porre in essere adeguati rimedi, occorre definire progetti specifici.
ALTO	Situazione con deficienze diffuse e talvolta non completamente note. Non conformità alle norme di legge. Il livello di protezione è discontinuo e inefficace. Per porvi rimedio è necessario impostare progetti impegnativi, in termini di risorse umane ed economiche.

Di seguito si riporta una sintetica analisi dei rischi secondo le diverse aree analizzate:

Area	Situazione riscontrata	Livello di rischio
Politica della sicurezza	Documento Programmatico sulla Sicurezza aggiornato e con indicazione delle politiche della sicurezza volute dall'Ente.	basso
Organizzazione della sicurezza	Ruolo del Responsabile della sicurezza formalmente assegnato. Alcuni ruoli tecnici risultano assegnati di fatto, ma non ancora formalizzati.	medio
Classificazione e controllo	Procedura di individuazione e classificazione dei dati non presente.	medio
Condotta del personale	Pianificazione training per il personale dipendente da definire. Politica di clean desk non sostenuta.	medio
Sicurezza fisica e ambientale	Accesso agli uffici non controllato da guardiania. Procedure di controllo e gestione accessi non formalizzate	medio
Gestione dei computer e della rete	Processi di system management carenti. Configurazione rete e sistemi da adeguare. Gestione user-ID e password da implementare.	medio - alto
Procedure di accesso	Procedure e profili di accesso non formalizzati. Carenza di controlli periodici.	medio - alto
Piano di continuità	Backup non sistematici e frequenti. Piano di continuità non presente.	medio - alto
Archivi cartacei	Carente politica di clean desk. Gestione accesso archivi presente di fatto, ma non formalizzata.	medio
Gestione workstation	Piattaforma non centralizzata. Assenza di un server di rete e di un server di backup. Antivirus non presenti su ogni postazione e non aggiornati in modo sistematico. Carente protezione dati personali su archivi locali.	medio - alto
Servizi in outsourcing	Norme di sicurezza e responsabilità formalizzate.	basso

6. Prescrizioni di sicurezza

Obiettivo di tali prescrizioni è definire le regole fondamentali per la realizzazione delle misure di sicurezza per le informazioni personali e dell'Ente oggetto di trattamento.

Sono da considerarsi eccezioni, rispetto a quanto di seguito disciplinato, i sistemi isolati (non in rete) che non contengono dati personali e/o del Consorzio.

I dati personali, comuni e sensibili, devono essere messi a disposizione solo delle persone che hanno la necessità di accedervi per fini di trattamento. L'accesso deve

essere esplicitamente permesso solo con le modalità previste dal trattamento e limitato ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.
Le autorizzazioni di accesso devono risultare da appositi documenti.
Di norma, le risorse del sistema operativo sono accessibili agli utenti ordinari in modalità di sola lettura o esecuzione. Fanno eccezione quelle risorse che, se conosciute, potrebbero consentire di aggirare i sistemi di sicurezza (ad es. log, archivi contenenti le password, etc.). Queste risorse sono inaccessibili all'utenza ordinaria.
Ogni sistema e/o banca dati contenente dati personali o dell'Ente, deve essere dotata di una funzione di identificazione ed autenticazione basata su user-ID e password.
Ogni user-ID deve essere univocamente e direttamente associato ad un singolo utente. La user-ID è costituita secondo le regole in vigore. Una volta assegnata ad una persona, la user-ID non deve essere più oggetto di assegnazione, anche in tempi diversi, ad altra persona. E' compito del Responsabile del trattamento definire una procedura per garantire il rispetto di questa norma.
Il Responsabile del trattamento rilascia l'user-ID, che permette l'accesso alle banche dati ed alla rete, utilizzando l'apposita procedura.
Quando un incaricato non ha più la necessità di accedere ad una banca dati, o lascia il Consorzio, il Responsabile del trattamento deve chiedere, tempestivamente, di disabilitare l'utenza non più necessaria. Le user-ID non utilizzate per un periodo superiore a sei mesi devono, a cura del Responsabile, essere disabilitate. Fanno eccezione le user-ID di manutenzione che non scadono mai.
In caso di nomina di un *amministratore di sistema*, le seguenti responsabilità, facenti capo al Responsabile del trattamento, vengono a lui trasferite:

- sovrintendere alle risorse dei sistemi operativi degli elaboratori;
- sviluppare, realizzare e mantenere aggiornate, per le banche dati gestite con sistemi informatici, le misure di sicurezza in accordo con le norme contenute nel presente documento;
- fornire guida e supporto agli Incaricati;
- amministrare e gestire la sicurezza informatica operando, se necessario, anche come gestore delle password;

- nell'ambito delle responsabilità assegnate, effettuare periodici controlli e verifiche tecniche in merito al rispetto delle prescrizioni contenute nel presente documento.

Personale non direttamente dipendente dal Consorzio può essere utilizzato per le attività connesse con il servizio di elaborazione dati. In tal caso non sono richieste ulteriori misure di sicurezza oltre quelle descritte nel presente documento. Tuttavia, nel caso in cui tali risorse siano nella posizione di accedere a informazioni personali o riservate, ovvero ai sistemi o alla rete interna eludendo i sistemi di controllo, è richiesta la preventiva approvazione del Responsabile del trattamento per il loro intervento.

A solo titolo di esempio si elencano i ruoli tipici che hanno la possibilità di eludere i sistemi di controllo:

- personale che utilizza utenze privilegiate di sistema;
- personale che utilizza utenze privilegiate per la manutenzione hardware e software;
- personale che utilizza utenze privilegiate per la manutenzione delle librerie applicative.

Il Responsabile del trattamento deve, con cadenza annuale, procedere alla convalida dei diritti di accesso sotto la propria responsabilità.

Computer, supporti di dati e simili devono essere smaltiti correttamente per evitare che vengano cestinate o divulgate involontariamente informazioni personali c.d. "residue".

Sono definite "informazioni residue" quei dati personali ancora leggibili dopo la cessazione di un trattamento (ad es. floppy disk, compact disk, nastri magnetici, ecc).

I dati personali e del Consorzio "riservati" devono essere resi illeggibili prima del riutilizzo dei supporti in un altro trattamento o prima dell'alienazione dei supporti stessi.

E' compito del Responsabile del trattamento (o dell'amministratore di sistema, ove nominato) definire e tenere aggiornate procedure interne che disciplinino le appropriate modalità di cancellazione secondo i supporti utilizzati.

Fermo restando il posizionamento logistico di stampanti e fax, secondo quanto indicato al punto 3 del presente Documento, 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 del Consorzio "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.

7. Criteri e modalità di ripristino della disponibilità dei dati

E' fissata in 7 giorni la frequenza minima per i backup di tutte le banche dati gestite dal Consorzio.

E' compito del Responsabile dei trattamenti (o dell'amministratore di sistema, ove nominato) effettuare periodicamente una copia di backup dei dati personali e delle informazioni in genere gestite dal Consorzio.

I supporti di backup devono essere prontamente riposti nei locali/armadi appositamente predisposti. Con cadenza mensile, i supporti devono essere trasferiti in locali separati situati in un piano diverso da quello in cui sono presenti gli archivi originali.

Con cadenza almeno annuale, il Responsabile dei trattamenti deve predisporre un test per verificare la capacità di rilettura dei supporti e la ricostruzione delle banche dati.

Il backup deve essere effettuato anche per i dati personali o del Consorzio presenti sulle Workstation degli Incaricati al trattamento.

A cura del Responsabile dei trattamenti devono essere predisposte opportune procedure per assicurare la ripresa del servizio informatico in tempi e con livelli adeguati alla criticità delle operazioni automatizzate. Il tempo minimo di ripristino, per i trattamenti con dati sensibili, non deve essere superiore a 7 giorni.

Il furto o il danneggiamento delle apparecchiature informatiche, la diffusione o distruzione non autorizzata di informazioni e l'interruzione dei processi informatici, oltre che a danneggiare il Consorzio, possono esporre il Titolare dei trattamenti delle informazioni personali al rischio di violazioni di legge. Per tale motivo sono istituiti controlli per limitare l'accesso fisico ad alcune aree, così come indicato al punto 3 del presente Documento.

8. Pianificazione degli interventi formativi

Allo scopo di rendere edotti Responsabili e incaricati del trattamento dei rischi che incombono sui dati, della disciplina vigente in materia di privacy e delle responsabilità che ne derivano, l'Ente si occuperà della formulazione di un adeguato piano di formazione che vedrà i suoi momenti attuativi:

- al momento dell'ingresso in servizio;
- in occasione dei cambiamenti di mansione;
- in occasione dell'introduzione di nuovi strumenti e programmi informatici.

9. Trattamenti affidati all'esterno

In caso di trattamenti affidati all'esterno (ad es. società Sigma), la società, l'ente o la persona fisica a cui viene affidato il trattamento deve rilasciare specifiche dichiarazioni o documenti, oppure assumere alcuni impegni anche su base contrattuale, con particolare riferimento, ad esempio, a:

- trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
- adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
- impegno a informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

Oltre a prevedere contrattualmente un obbligo generale di riservatezza, deve essere previsto anche un obbligo specifico, a carico della società a cui viene affidato il trattamento, di adottare misure tecnologiche che impediscano l'accesso nella rete da parte di terzi estranei. A tali obblighi contrattuali la società potrà assolvere adottando le seguenti soluzioni:

- programmi "firewall", software che filtrano la trasmissione dei dati tra rete aziendale e rete esterna (Internet), intercettandoli e verificando se rispettino i requisiti stabiliti dall'amministratore di rete;
- gestire i dati dell'azienda/ente cliente non in linea, ovvero su una rete intranet protetta;
- adottare una policy interna per la gestione dei dati, un protocollo cioè che i dipendenti dovranno seguire nello svolgimento delle attività delegate, ad esempio vietando la duplicazione delle informazioni sui propri terminali e nelle cartelle condivise in rete e prescrivendo la loro sistematica cancellazione al termine delle operazioni.

Tutte le attività affidate in outsourcing devono in ogni caso rispettare le regole del presente D.P.S. e copia dello stesso deve essere allegata al contratto di servizio e farne parte a tutti gli effetti.

10. Revisione del Documento Programmatico sulla Sicurezza

Il presente Documento Programmatico sulla Sicurezza è valido per un anno. Trascorso tale termine deve essere oggetto di revisione, a cura del Responsabile della Sicurezza, 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.