C.F.P. CONSORZIO ENFAPI TREVIGLIO

Cod. Fiscale e Partita IVA 01281810166

Sede: Via Nenni,4 - 24047 TREVIGLIO (BG)
Tel. 036349296 - 036347034 Fax 0363595531
mail: enfapitreviglio@confindustriabergamo.it

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

Rev. 31/03/15

Preambolo

Il presente documento viene redatto ai sensi dell'articolo 34 lettera g) del D. Lgs. 196/2003, denominato "Testo Unico per la Protezione dei Dati Personali" (nel seguito "T.U."), per definire le misure "idonee" di sicurezza che CONSORZIO ENFAPI TREVIGLIO (nel seguito indicata come "l'Ente") intende adottare per garantire la riservatezza del trattamento dei dati personali e l'integrità dei sistemi informativi.

Il documento è strutturato in sezioni che seguono la struttura delineata all'articolo 19, allegato B del T.U.:

1. Elenco dei trattamenti dei dati personali: comprende l'elenco di tutti i trattamenti effettuati, delle risorse e delle applicazioni utilizzate, delle modalità di trattamento e dei loro ambiti di comunicazione; profili di autorizzazione degli incaricati
2. Analisi dei rischi relativi ai dati e ai metodi di trattamento (accesso ed uso non autorizzato, indisponibilità, non integrità)
3. Individuazione delle misure idonee a prevenire i rischi di cui al punto precedente, sia a livello informatico che fisico e procedurale; include anche i criteri e le modalità per il ripristino dei dati in caso di incidente (archivi di backup e procedure per l'esecuzione, per il ripristino e per la verifica)
4. Distribuzione dei compiti e delle responsabilità relative alla gestione dei sistemi di sicurezza e all'aggiornamento del presente documento
5. Programmazione degli interventi formativi e motivazionali ad uso del personale
6. Criteri per la gestione di dati trattati all'esterno di CONSORZIO ENFAPI TREVIGLIO: documentazione della necessità e della modalità di comunicazione, ed acquisizione del documento programmatico e delle dichiarazioni di adozione delle misure di sicurezza
7. Criteri di cifratura e gestione separata per i dati sensibili
8. Procedure adeguate di verifica per tutto quanto previsto dal Documento.

Il presente documento viene adottato mediante una delibera del Legale Rappresentante, e contestualmente a tale atto vengono designati tutti i funzionari con incarichi speciali collegati a questo documento, secondo quanto specificato al capitolo 4

Contestualmente viene approvato anche il "Manuale di sicurezza ad uso degli incaricati" che è allegato al presente Documento. I documenti e le designazioni sostituiscono e abrogano gli analoghi documenti e provvedimenti già in vigore.

.

1 Elenco dei trattamenti

1.1 Individuazione dei trattamenti effettuati

1.1.1 Archivio dati clienti (aziende, aziende associate, enti committenti)

I dati, presenti negli archivi in formato elettronico e/o cartaceo, sono relativi a clienti dell'Ente e riguardano sia i contatti, sia le informazioni contabili e fiscali relative agli ordini ed ai pagamenti. **Si tratta solamente di dati personali**.

Finalità del trattamento

I dati vengono trattati al fine di assicurare un corretto funzionamento dell'Ente e di dare corso agli ordini dei clienti stessi.

Informativa e consenso

I dati vengono trattati al fine di dare esecuzione a un ordine impartito dall'interessato e da lui sottoscritto e pertanto non è richiesta la prestazione esplicita del consenso, ai sensi dell'art. 24 comma 1 lettere a) b) d) .
L'informativa, resa ai sensi dell'art. 13 (mod. *PRI01 Informativa CLIENTI_FORNITORI SENZA firma CONSENSO* inserito tra gli allegati al DPS), è inviata ai clienti (nuovi e storici) tramite fax oppure effettuata oralmente in ogni altro caso,.

Modalità di trattamento

I dati in formato elettronico vengono trattati dal personale dell'Ente per le operazioni giornaliere: il personale è identificato mediante procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. I dati in formato cartaceo vengono trattati dal personale dell'Ente per le operazioni giornaliere secondo le modalità espresse al successivo paragrafo 3.2.5.

Ambiti di comunicazione e diffusione

I dati personali dei clienti non vengono comunicati né diffusi all'esterno se non al Rag. ROGNONI e/o allo Studio VERONELLI che gestiscono le elaborazioni contabili e le dichiarazioni fiscali di legge.
I dati personali dei clienti relativi ad eventuali corsi finanziati (es. aziende di appartenenza degli apprendisti) vengono trattati tramite portali messi a disposizione online da Regione Lombardia , Provincia di Bergamo o da altri Enti finanziatori.

Profili di autorizzazione degli incaricati

Sono stati definiti dei Profili di autorizzazione personalizzati per ciascun utente dell'Ente (procedura di autenticazione e autorizzazione rispondente ai requisiti delineati ai successivi paragrafi 3.3.4-3.3.5) in modo da garantire ad ognuno un accesso ai dati limitato alla competenza di autorizzazione necessaria al corretto svolgimento della propria mansione aziendale .

Applicazioni utilizzate

Al fine della gestione dei dati personali dei clienti in formato elettronico viene utilizzato un applicativo gestionale fornito in outsourcing da Zucchetti S.p.A. "*Gestionale 1*" ma anche un applicativo interno realizzato in ACCESS "*ENFAPI.mdb*" e banche dati in formato Excel.

Modalità di conservazione dei dati

I dati in formato elettronico vengono conservati su una macchina SERVER, e possono essere acceduti al personale dell'Ente soltanto mediante una procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. I dati cartacei sono conservati in armadi chiusi a chiave così come delineato al successivo paragrafo 3.2.5.

1.1.2 Archivio Allievi

I dati sono relativi agli allievi iscritti ai corsi: **si tratta di dati personali e sensibili, e di dati didattici**.

1.1.2.1 Archivio Allievi: dati personali e sensibili

Finalità del trattamento

I dati, presenti negli archivi sia in formato elettronico che in formato cartaceo, vengono trattati al fine di assicurare un corretto funzionamento dell'Ente e al fine di dare corso all'attività formativa alla quale gli allievi risultano iscritti.
Il CONSORZIO ENFAPI TREVIGLIO dichiara che non tratta i dati sensibili, relativi delle disabilità e agli aspetti medici degli allievi, che verranno quindi conservati in un protocollo riservato, archiviato a cura del Responsabile del Trattamento in un armadio chiuso a chiave.

Informativa e consenso

I dati vengono trattati al fine di dare esecuzione a un ordine impartito dall'interessato: è richiesta la prestazione esplicita del consenso ai sensi dell'art. 24 comma 1 lettere a) b) d) .
L'informativa, resa ai sensi dell'art. 13 (mod. *PRI02 Informativa ALLIEVI CON firma CONSENSO* inserito tra gli allegati al DPS) viene data agli allievi all'atto della formalizzazione dell'iscrizione all'azione formativa ed è effettuata oralmente in ogni altro caso.

Modalità di trattamento

I dati in formato elettronico vengono trattati dal personale dell'Ente per le operazioni giornaliere: il personale è identificato mediante procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. I dati in formato cartaceo vengono trattati trattati dal personale dell'Ente per le operazioni giornaliere secondo le modalità espresse al successivo paragrafo 3.2.5.

Ambiti di comunicazione e diffusione

I dati personali degli allievi non vengono comunicati né diffusi all'esterno eccetto per:

- Studio VERONELLI che gestisce l'elaborazione dei compensi delle risorse umane per eventuali importi da erogare, in particolari casi, agli allievi.
- al Rag. ROGNONI che gestisce le elaborazioni contabili e le dichiarazioni fiscali di legge.
- alla Regione Lombardia , alla Provincia di Bergamo o da altri Enti finanziatori trattati tramite portali da loro stessi messi a disposizione online
- alle aziende per l'effettuazione di stage o per eventuali successive assunzioni.
- all'INAIL, alla Direzione Provinciale del Lavoro e all'INPS ai fini della gestione degli stage formativi aziendali

Si ricorda che in nessun caso vengono comunicati o diffusi i dati relativi alla disabilità degli allievi.

Profili di autorizzazione degli incaricati

Sono stati definiti dei Profili di autorizzazione personalizzati per ciascun utente dell'Ente (procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5) in modo da garantire ad ognuno un accesso ai dati limitato alla competenza di autorizzazione necessaria al corretto svolgimento della propria mansione aziendale.

Applicazioni utilizzate

Al fine della gestione dei dati personali degli allievi in formato elettronico viene utilizzato un applicativo gestionale fornito in outsourcing da Zucchetti S.p.A. "*Gestionale 1*" ma anche un applicativo interno realizzato in ACCESS "*ENFAPI.mdb*". (applicativi gestionali Microsoft: WORD e EXCEL).

Modalità di conservazione dei dati

I dati in formato elettronico vengono conservati su una macchina SERVER, e possono essere acceduti al personale dell'Ente soltanto mediante una procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. I dati cartacei sono conservati in armadi chiusi a chiave così come delineato al successivo paragrafo 3.2.5..
I dati in formato elettronico o in formato cartaceo che attestano eventuali disabilità degli allievi verranno conservati a cura del Responsabile del Trattamento in armadi chiusi a chiave. Nello stesso armadio verranno conservati i documenti di scelta relativa alla frequenza delle ore di religione Cattolica.

1.1.2.2 Archivio Allievi: dati didattici

Finalità del trattamento

I dati didattici, presenti negli archivi sia in formato elettronico che in formato cartaceo,vengono trattati al fine di assicurare una corretta valutazione degli allievi.

Informativa e consenso

I dati vengono trattati al fine di produrre valutazioni degli allievi da inserire nel PORTFOLIO, nel libretto di valutazione o nelle certificazioni delle competenze: è richiesta la prestazione esplicita del consenso ai sensi dell'art. 24 comma 1 lettere a) b) d) .
L'informativa, resa ai sensi dell'art. 13 (mod. *PRI02 Informativa ALLIEVI CON firma CONSENSO* inserito tra gli allegati al DPS) viene data agli allievi all'atto della formalizzazione dell'iscrizione all'azione formativa ed è effettuata oralmente in ogni altro caso

Modalità di trattamento

I dati in formato elettronico vengono trattati dal personale dell'Ente per le operazioni giornaliere: il personale è identificato mediante procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. I dati in formato cartaceo vengono trattati secondo le modalità espresse al successivo paragrafo 3.2.5.

Ambiti di comunicazione e diffusione

I dati didattici degli allievi non vengono comunicati né diffusi all'esterno eccetto per:

- Il dati relativi al Porfolio, al libretto di valutazione e alle valutazioni

periodiche verranno comunicati agli esercenti la patria potestà durante il corso e a fine corso.
- I dati relativi alla Certificazione delle Competenze/abilità/conoscenze che, nel caso di corsi per Apprendisti e di Formazione Continua, potranno essere diffusi anche alle aziende di appartenenza.
- I dati relativi alla Certificazione delle Competenze/abilità/conoscenze nel caso dei corsi di Qualifica in DDIF, di Diploma di quarto anno, di Formazione Superiore saranno inseriti anche nelle banche dati Regione Lombardia.

Profili di autorizzazione degli incaricati

Sono stati definiti dei Profili di autorizzazione personalizzati per ciascun utente dell'Ente (procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5) in modo da garantire ad ognuno un accesso ai dati limitato alla competenza di autorizzazione necessaria al corretto svolgimento della propria mansione aziendale..

Applicazioni utilizzate

Al fine della gestione dei dati didattici degli allievi in formato elettronico vengono utilizzati applicativi Microsoft: WORD e EXCEL

Modalità di conservazione dei dati

I dati in formato elettronico vengono conservati su una macchina SERVER, e possono essere acceduti al personale dell'Ente soltanto mediante una procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. I dati cartacei sono conservati in armadi chiusi a chiave così come delineato al successivo paragrafo 3.2.5..

1.1.3 Archivio dati fornitori (aziende fornitrici di beni e/o servizi, aziende associate, aziende stage)

I dati, presenti negli archivi in formato elettronico e/o cartaceo, sono relativi ai fornitori dell'Ente e riguardano sia i contatti, sia le informazioni contabili e fiscali relative agli ordini ed ai pagamenti. **Si tratta solamente di dati personali**.

Finalità del trattamento

I dati vengono trattati al fine di assicurare un corretto funzionamento dell'Ente e di dare corso agli ordini dati ai fornitori stessi.

Informativa e consenso

I dati vengono trattati al fine di dare esecuzione a un ordine impartito all'interessato e da lui sottoscritto e pertanto non è richiesta la prestazione esplicita del consenso, ai sensi dell'art. 24 comma 1 lettere a) b) d) .
L'informativa resa ai sensi dell'art. 13 (mod. *PRI01 Informativa CLIENTI_FORNITORI SENZA firma CONSENSO* inserito tra gli allegati al DPS), è inviata ai fornitori (nuovi e storici) tramite fax oppure effettuata oralmente in ogni altro caso,

Modalità di trattamento

I dati in formato elettronico vengono trattati dal personale dell'Ente per le operazioni giornaliere: il personale è identificato mediante procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5.
I dati in formato cartaceo vengono trattati dal personale dell'Ente per le operazioni giornaliere secondo le modalità espresse al successivo paragrafo

3.2.5.

Ambiti di comunicazione e diffusione

I dati personali dei fornitoti non vengono comunicati né diffusi all'esterno, se non al Rag. ROGNONI e allo Studio VERNELLI che gestiscono le elaborazioni contabili e le dichiarazioni fiscali di legge.
I dati personali dei fornitori relativi ad eventuali corsi finanziati vengono trattati tramite portali messi a disposizione online da Regione Lombardia , Provincia di Bergamo o da altri Enti finanziatori.

Profili di autorizzazione degli incaricati

Sono stati definiti dei Profili di autorizzazione personalizzati per ciascun utente dell'Ente (procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5) in modo da garantire ad ognuno un accesso ai dati limitato alla competenza di autorizzazione necessaria al corretto svolgimento della propria mansione aziendale.

Applicazioni utilizzate

Al fine della gestione dei dati personali dei fornitori in formato elettronico viene utilizzato un applicativo gestionale fornito in outsourcing da Zucchetti S.p.A. "*Gestionale 1*" ma anche un applicativo interno realizzato in ACCESS "*ENFAPI.mdb*"

Modalità di conservazione dei dati

I dati in formato elettronico vengono conservati su una macchina designata SERVER e possono essere acceduti al personale dell'Ente soltanto mediante una procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. I dati cartacei sono conservati in armadi chiusi a chiave così come delineato al successivo paragrafo 3.2.5.

1.1.4 Archivio dati risorse umane (interne ed esterne)

I dati, presenti negli archivi in formato elettronico e/o cartaceo, sono relativi alle risorse umane dell'Ente e riguardano i dati contenuti nel curriculum vitae e negli eventuali allegati allo stesso. **Si tratta sia di dati personali che di dati sensibili (**in quanto il curriculum vitae potrebbe contenere dati indicativi delle condizioni di salute della risorsa umana, la sua eventuale iscrizione ad albi sindacali oppure contenere possibili riferimenti all'etnia o alla convinzione religiosa).
N.B. ad oggi i curriculum vitae non contengono dati sensibili.

Finalità del trattamento

I dati vengono trattati al fine di assicurare un corretto funzionamento dell'Ente ovvero al fine di progettare, promuovere, programmare, realizzare e monitorare l'attività formativa svolta dall'Ente.

Informativa e consenso

I dati vengono trattati al fine di dare esecuzione a un ordine impartito dall'Ente per la realizzazione dell'attività formativa: è richiesta la prestazione esplicita del consenso, ai sensi dell'art. 24 comma 1 lettere a) b) d) .
L'informativa, resa ai sensi dell'art. 13 (mod. *PRI03 Informativa RISORSE UMANE CON firma CONSENSO* inserito tra gli allegati al DPS), viene data alle risorse umane in sede di sottoscrizione del contratto oppure effettuata oralmente in ogni altro caso,

Modalità di trattamento

I dati in formato elettronico vengono trattati dal personale dell'Ente per le operazioni giornaliere: il personale è identificato mediante procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. I dati in formato cartaceo vengono trattati dal personale dell'Ente per le operazioni giornaliere secondo le modalità espresse al successivo paragrafo 3.2.5.

Ambiti di comunicazione e diffusione

I dati personali e sensibili delle risorse umane non vengono comunicati né diffusi all'esterno, se non al Rag. ROGNONI e allo Studio VERONELLI che gestiscono le elaborazioni contabili e le dichiarazioni fiscali di legge.
I dati personali e sensibili delle risorse umane riferibili ad eventuali corsi finanziati vengono trattati tramite portali messi a disposizione online da Regione Lombardia , Provincia di Bergamo o da altri Enti finanziatori. .

Profili di autorizzazione degli incaricati

Sono stati definiti dei Profili di autorizzazione personalizzati per ciascun utente dell'Ente (procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5) in modo da garantire ad ognuno un accesso ai dati limitato alla competenza di autorizzazione necessaria al corretto svolgimento della propria mansione aziendale.

Applicazioni utilizzate

Al fine della gestione dei dati personali delle risorse umane in formato elettronico viene utilizzato un applicativo gestionale fornito in outsourcing da Zucchetti S.p.A. "*Gestionale 1*" ma anche un applicativo interno realizzato in ACCESS "*ENFAPI.mdb*"

Modalità di conservazione dei dati

I dati in formato elettronico vengono conservati su una macchina designata SERVER e possono essere acceduti al personale dell'Ente soltanto mediante una procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. I dati cartacei sono conservati in armadi chiusi a chiave così come delineato al successivo paragrafo 3.2.5.

1.1.5 Archivi di indirizzi e-mail

I dati si riferiscono ai clienti ed ai fornitori dell'Ente e riguardano i contatti e-mail.

Finalità del trattamento

I dati vengono trattati al fine di mantenere le comunicazioni con clienti e fornitori promuovendo così l'attività formativa dell'Ente sia in termini di proposte corsuali che in termini di proposte stage.

Informativa e consenso

L'informativa resa ai sensi dell'art. 13 (mod. *PRI01 Informativa CLIENTI_FORNITORI SENZA firma CONSENSO* inserito tra gli allegati al DPS), è inviata ai fornitori (nuovi e storici) tramite fax/mail oppure effettuata oralmente in ogni altro caso,

Modalità di trattamento

I dati vengono trattati ed aggiornati costantemente dal personale dell'Ente per le operazioni giornaliere: il personale è identificato mediante procedura di

autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5.. I dati possono venire utilizzati per l'invio di comunicazioni pubblicitarie.

Ambiti di comunicazione e diffusione

I dati mail non vengono né comunicati né diffusi all'esterno di CONSORZIO ENFAPI TREVIGLIO. I dati possono venire comunicati, esclusivamente al fine di dar corso ad espresse richieste del soggetto a cui i dati si riferiscono e agli enti preposti dalla legge.

Profili di autorizzazione degli incaricati

Solo alcuni profili di autorizzazione abilitano ad accedere agli indirizzi di posta elettronica oltre ad essere stati definiti dei Profili di autorizzazione personalizzati per ciascun utente dell'Ente (procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5) in modo da garantire ad ognuno un accesso ai dati limitato alla competenza di autorizzazione necessaria al corretto svolgimento della propria mansione aziendale .

Applicazioni utilizzate

Al fine della gestione dei dati mail di clienti e fornitori viene utilizzato l'applicativo "*LOTUS NOTES*".

Modalità di conservazione dei dati

I dati sono conservati su un SERVER esterno gestito da CONFINDUSTRIA BERGAMO.

1.1.6 Archivio dati paghe – contributi

I dati sono relativi agli elementi necessari per l'elaborazione delle paghe e dei contributi dei lavoratori dell'Ente. **Si tratta sia di dati personali che di dati sensibili** (in quanto indicativi ad esempio delle condizioni di salute, o l'iscrizione sindacale del lavoratore) ..

Informativa e consenso

I dati vengono trattati al fine di elaborare i compensi delle risorse umane e di provvedere alle relative dichiarazioni fiscali previste dalla legge: è richiesta la prestazione esplicita del consenso.L'informativa, resa ai sensi dell'art. 13 (mod. *PRI03 Informativa RISORSE UMANE CON firma CONSENSO* inserito tra gli allegati al DPS) viene data alle risorse umane in sede di sottoscrizione del contratto oppure effettuata oralmente in ogni altro caso,.

Modalità di trattamento

I dati vengono raccolti all'interno dell'Ente, conservati ed archiviati e trasferiti per l'elaborazione allo Studio VERONELLI, che agisce in modo indipendente fornendo i risultati dell'elaborazione all'Ente, configurando pertanto un trattamento di dati autonomo.

Ambiti di comunicazione e diffusione

I dati necessari per l'elaborazione delle paghe e dei contributi delle risorse umane non vengono comunicati né diffusi all'esterno, se non allo Studio VERONELLI.

Profili di autorizzazione degli incaricati

Sono stati definiti dei Profili di autorizzazione personalizzati per ciascun

utente dell'Ente (procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5) in modo da garantire ad ognuno un accesso ai dati limitato alla competenza di autorizzazione necessaria al corretto svolgimento della propria mansione aziendale..

Applicazioni utilizzate

Al fine della gestione dei dati personali delle risorse umane in formato elettronico viene utilizzato un applicativo gestionale fornito in outsourcing da Zucchetti S.p.A. "*Gestionale 1*" ma anche un applicativo interno realizzato in ACCESS "*ENFAPI.mdb*" . Al fine della trasmissione dei dati allo Studio VERONELLI vengono utilizzate applicazioni Microsoft nonché l'applicativo"*LOTUS NOTES*". .

Modalità di conservazione dei dati

I dati vengono raccolti e conservati dal soggetto terzo (Studio VERONELLI) sotto contratto con CONSORZIO ENFAPI TREVIGLIO.
Tuttavia il CONSORZIO ENFAPI TREVIGLIO conserva anch'egli i dati in formato elettronico su una macchina designata SERVER e possono essere acceduti al personale dell'Ente soltanto mediante una procedura di autenticazione e autorizzazione rispondente ai requisiti delineati al successivo paragrafo 3.3.4-3.3.5. Provvede inoltre a conservare anche i dati cartacei in armadi chiusi a chiave così come delineato al successivo paragrafo 3.2.5.
.

1.2 Luoghi fisici coinvolti

La conservazione e il trattamento dei dati avviene principalmente nella sede dell'Ente, sita in Via P. Nenni, Treviglio, e presso lo Studio VERONELLI sito in Via C. Abba 4 Bergamo.

1.3 Risorse hardware utilizzate

Viene utilizzato per la conservazione e il trattamento dei dati in formato elettronico un SERVER, oltre a stazioni desktop, sito nella sede dell'Ente.

Un elenco aggiornato delle macchine utilizzate per il trattamento dei dati personali è descritto nell'*allegato D* parte 1) del presente documento.

2 Analisi dei rischi

2.1 Introduzione e metodologia

Il T.U. indica il documento programmatico sulla sicurezza come lo strumento per identificare, valutare e contrastare i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta, o della presenza di errori nei dati stessi. Non si può certo pretendere di essere esaustivi in tale analisi, ma si possono delineare i rischi peggiori.

Gli elementi per la valutazione del rischio sono:
- La *probabilità* che l'evento dannoso accada
- La potenziale *dannosità* dell'evento, in tre specifiche direzioni
  - alterazione dei dati
  - accesso non autorizzato o non conforme
  - distruzione o perdita dei dati

Per ogni tipologia di rischio saranno valutate la probabilità e la dannosità su scale da 1 a 4, come dalle tabelle seguenti:

Livello	Probabilità
1	Quasi impossibile
2	Raro
3	Frequente
4	Frequentissimo

Livello	Dannosità
1	Lieve
2	Media
3	Grave
4	Gravissima

I danni di entità lieve (rischio molto basso corrispondente ad una minaccia remota e comunque rapidamente reversibile od ovviabile) sono sicuramente da evitare, ma possono essere contenuti ed eventualmente riparati mediante procedure prestabilite. Danni di media entità (rischio superiore al precedente corrispondente ad una minaccia remota ma i cui effetti non sono facilmente o totalmente reversibili od ovviabili) sono danni lievi ma molto estesi, oppure danni solo parzialmente reversibili. Danni gravi e gravissimi (rischio che occorre assolutamente prevenire per abbatterlo e contenerlo) sono inaccettabili, e non possono essere riparati, o possono esserlo solo con costi proibitivi.

2.2 Rischi fisici

I rischi fisici possono riguardare sia i luoghi (e con essi i supporti cartacei utilizzati per il trattamento dei dati) che le risorse hardware (entrambi individuati al precedente paragrafo 1.2 e 1.3). L'Ente è dotato di un servizio di videosorveglianza interno cosi come descritto nell'*Allego F*.

Per quanto riguarda i luoghi, individuati al precedente paragrafo 1.2, alcuni rischi possibili sono:
- *Intrusione forzata all'interno delle sedi*: potenzialmente il danno sarebbe grave, se non gravissimo. Tuttavia, con l'uso corretto di chiavi, la probabilità è ridotta a raro. La sede è protetta da allarme antiintrusione e da servizio di vigilanza.
- *Accesso di persone non autorizzate*: l'accesso di persone non autorizzate ad aree e documenti riservati può avvenire con grande difficoltà data la

struttura, ,la disposizione degli uffici e la presenza di armadi provvisti di serratura (probabilità Raro). I possibili danni sono sicuramente gravi.

- *Allagamento*: la posizione della sede indica scarsa probabilità di allagamenti naturali mentre rimane ovviamente possibile un allagamento parziale provocato da danni a condotte e impianti. La dannosità probabilmente media e la rara, se non rarissima, e l'eventuale frequenza dell'evento inducono a considerarlo un rischio secondario. Vengono conservate all'esterno copie del backup mensile dei dati in formato elettronico
- *Incendio e/o esplosione*: esiste una possibilità di incendio all'interno della struttura (evento Rarissimo, con possibili danni Gravi o Gravissimi), mentre appare remota la possibilità di un'esplosione. Vengono controllati gli impianti rivelatori ed estintori di incendi, e vengono conservate all'esterno copie del backup mensile dei dati in formato elettronico. Si è inoltre provveduto a dotarsi di cassette di sicurezza ignifughe.

2.3 Rischi telematici

Per quanto riguarda i sistemi elettronici, e quindi le risorse hardware individuate al precedente paragrafo 1.3, alcuni rischi possibili sono:

- *Intrusione*: potenzialmente il danno sarebbe grave. Tuttavia, giudichiamo la probabilità rara, in quanto pochi dei servizi dell'Ente sono esposti verso la rete Internet.
- *Contaminazione da virus*: il rischio potenziale è grave, e la minaccia frequente. L'adozione di adeguate misure antivirus è prioritaria.
- *Guasto hardware-software*: l'evento può oscillare tra un danno medio e gravissimo, ed è raro. Tuttavia l'adozione di adeguate procedure di backup dei dati in formato elettronico può facilmente ridurre il danno a lieve-medio. Non risulta che danni da guasto possano paralizzare l'attività d'Ente

L'utilizzo limitato di software non standard consente di ritenere limitate le probabilità di introduzione di troiani, inoltre la politica di installazione del software sulle macchine aziendali è resa sufficientemente restrittiva.

3 Individuazione delle misure idonee

3.1 Introduzione

In questo capitolo si proporrà la **Politica di Sicurezza dell'Ente**: verrà cioè presentato *l'insieme delle misure fisiche, logiche ed organizzative* che si intende adottare per tutelare le strutture e gli strumenti, cartacei ed elettronici, preposti al trattamento dei dati.

A tale scopo è utile fare una premessa di tipo legislativo. Il T.U. riporta le norme per l'individuazione delle **misure minime di sicurezza** per il trattamento dei dati personali (Titolo II, art. 33 e seg.): se queste misure minime non fossero garantite, sono previste responsabilità penali (ex art. 169 T.U.).

Inoltre l'art. 31 recita che "I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da **ridurre al minimo,** mediante l'adozione di **idonee e preventive misure di sicurezza**, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

Le norme descritte in questa sezione del documento, pertanto, oltre ad applicare, per requisito di legge, le misure minime previste, cercano di individuare e di adottare misure idonee a prevenire i rischi delineati nella sezione precedente.

Gli Amministratori della Società, assieme al Titolare e ai Responsabili dei Trattamenti, stabiliscono i tempi e i metodi per l'attuazione di questo documento programmatico, entro gli ovvi limiti di spesa consentiti.

3.2 Sicurezza fisica dei locali, delle strutture e degli archivi

3.2.1 Protezione perimetrale

1. L'edificio è dotato di serrature su tutti i varchi di accesso dall'esterno. Durante l'orario di lavoro l'accesso all'edificio è controllato dal personale che controlla gli accessi di tutti i visitatori all'atto di apertura del portone della sede. Coloro che sono muniti delle chiavi dell'ufficio sono registrati nell'apposito *allegato A*. È fatto divieto a chiunque di trasferire copie delle chiavi (distribuite ai vari incaricati come da Mod. *PRI05 Registro assegnazione chiavi* inserito tra gli allegati al DPS) a persone che non siano inserite nell'*allegato A*.
2. Negli orari lavorativi le porte sono chiuse, ed il personale cura che i visitatori accedano agli uffici per ragioni valide.
3. Negli orari non lavorativi, le porte sono chiuse, ma possono essere aperte dai dipendenti che abbiano motivo di servizio per essere all'interno degli uffici.

3.2.2 Protezione degli uffici

1. Solo alcune stanze dell'Ente (segreteria didattica e amministrativa, sala SAME, ufficio del Direttore, ufficio Unione Industriali, archivio storico, aula Docenti) possono contenere documenti e sistemi elettronici con dati personali, e quindi sono soggette alle misure di protezione di seguito elencate.
2. I locali lavorativi vengono chiusi con cura dall'ultima persona che li lascia.
3. L'Ente è munito di armadi dotati di serratura in cui possono essere custoditi i documenti cartacei contenenti dati personali e/o dati sensibili. Tali documenti non devono essere custoditi al di fuori di detti armadi chiusi, se non per il tempo strettamente necessario al trattamento dei dati, e in nessun caso devono rimanere incustoditi.
4. L'impianto elettrico è verificato a norma di legge.
5. I supporti di backup dei dati, i dischi di installazione originali e tutti i supporti di memorizzazione conservati in sede vanno tenuti in armadi chiusi, distanti per quanto possibile dai computer. I supporti di backup di dati che contengono dati sensibili devono essere riposti in contenitori chiusi a chiave e non trasportabili (armadi blindati) preservandoli anche da eventuali rischi di incendio e/o esplosione (cassette di sicurezza ignifughe).

3.2.3 Protezione degli apparati di rete

1. Gli apparati di rete (es. SERVER) posizionati all'interno degli uffici devono essere, se possibile, chiusi a chiave in opportuni contenitori. Laddove ciò non fosse possibile dovranno essere posizionati in maniera tale da essere difficilmente raggiungibili senza che il personale delle stanze che li ospita lo noti. Le chiavi (distribuite ai vari incaricati come da Mod. *PRI05 Registro assegnazione chiavi* inserito tra gli allegati al DPS) e i rispettivi custodi saranno elencati nell'*allegato A*. Questa misura di protezione vale anche per il SERVER DIDATTICO (SERVERDID) posto in aula SONZOGNI anche se contiene solo file di esercitazione didattica degli allievi e protezioni per l'accesso a INTERNET e alle cartelle di altri allievi.
2. Laddove possibile le porte non utilizzate delle apparecchiature di rete sono disabilitate.

3.2.4 Protezione degli elaboratori elettronici

1. Il responsabile del trattamento mantiene un elenco, da aggiornare con cadenza almeno semestrale, di tutte le attrezzature informatiche degli uffici, lo scopo cui sono destinate, la loro locazione fisica, e se possibile l'indirizzo IP assegnato, che verrà inserito nel presente documento come dettagliato nell'*allegato D parte 1°*. Solo i computer eventualmente presenti nelle aule didattiche non seguono questa misura di protezione.
2. Gli elaboratori elettronici che trattano dati personali o sensibili sono disposti in locali protetti secondo quanto disposto al precedente punto 3.2.2.
3. Gli elaboratori portatili in uso all'interno degli uffici dovranno essere bloccati con gli appositi cavi di sicurezza laddove possibile. Durante le ore notturne, o comunque in assenza dell'utente, dovranno essere spenti e riposti in cassetti o armadi chiusi a chiave, oppure trasportati e sorvegliati a cura e responsabilità degli incaricati del trattamento.

4. Gli elaboratori portatili possono essere utilizzati per l'accesso e il trattamento temporaneo di dati personali o sensibili, ma non devono mai contenere, sulle unità disco locali, copie statiche di tali dati. Laddove necessario, questi dati possono essere conservati, ma esclusivamente in forma crittografata.
5. La mancanza di elaboratori, di loro parti, di supporti magnetici di memorizzazione o di materiale informatico di qualsiasi tipo, deve essere immediatamente segnalata a un amministratore di sistema e/o al responsabile o al titolare del trattamento.

3.2.5 Protezione degli archivi

1. I documenti cartacei vengono prelevati dagli archivi per il tempo necessario ad espletare il trattamento dei dati e/o il procedimento a cui sono connessi.
2. I documenti cartacei che non sono utilizzati devono essere archiviati o distrutti in modo sicuro mediante gli appositi distruggi documenti in dotazione.
3. I documenti cartacei giacenti ed abbandonati di cui non possa essere rintracciato l'autore saranno archiviati se possibile, oppure distrutti, a cura del Responsabile del Trattamento.
4. Gli archivi dati devono essere dotati di:
   - Impianto antincendio adeguato a locali contenenti carta;
   - Opportuni meccanismi di chiusura per i dati sensibili.
5. L'accesso agli archivi dati è consentito solo al responsabile del trattamento o alle persone espressamente autorizzate. L'apertura dell'archivio deve essere limitata al tempo strettamente necessario.
6. Oltre che per consentire quanto esplicitamente sopra autorizzato, gli archivi dei dati sensibili devono essere tenuti chiusi a chiave. La chiave è in possesso dei soggetti individuati dal Responsabile del Trattamento ed elencati nell'*allegato A e* distribuita ai vari incaricati come da Mod. *PRI05 Registro assegnazione chiavi* inserito tra gli allegati al DPS). Coloro che sono dotati delle chiavi sono responsabili della chiusura dell'archivio al di fuori di quanto stabilito al punto precedente. Si ricorda che l'Ente non tratta dati sensibili e quelli eventualmente in suo possesso vengono conservati a cura del responsabile del trattamento in contenitori chiusi a chiave e non trasportabili (armadi blindati).

3.3 Sicurezza logica ed integrità dei dati elettronici

3.3.1 Principio generale

Per ogni archivio elettronico, il responsabile del trattamento dei dati ha l'autorità di definire politiche di sicurezza **più restrittive** rispetto a quelle elencate nel presente documento, al fine di meglio tutelare le singole macchine e di adeguare il trattamento all'evolversi della tecnologia. Le eventuali norme e procedure aggiuntive per singole macchine saranno inserite come note nell'*allegato D*.

3.3.2 Sicurezza del software

1. È consentita l'installazione esclusiva delle seguenti tre categorie di software:
   - Software commerciale, dotato di licenza d'uso;

- Software libero, entro i termini della licenza pubblica d'uso;
- Software realizzato internamente.

2. L'installazione di ogni tipo di software va autorizzata preventivamente dal responsabile del trattamento e/o da un amministratore di sistema; il software, se utilizzato a giudizio del responsabile per trattare dati personali e/o dati sensibili, deve essere inserito nella cornice di questo documento programmatico in sede di revisione. L'elenco dei software approvati per il trattamento di dati personali è inserito nel presente documento come *allegato B*.
3. La conformità dei software utilizzati per il trattamento di dati personali a quanto disposto dal T.U. viene di norma certificata dal fornitore al Responsabile del Trattamento. Laddove ciò non fosse possibile, ne viene data notizia motivata nell'elenco di cui all'*allegato B*.
4. Il software deve essere installato solo da supporti fisici originali o dei quali sia nota la provenienza.
5. Laddove possibile, tutti i sistemi saranno impostati per l'installazione automatica degli aggiornamenti del software, con cadenza se possibile settimanale. In ogni caso, un incaricato nominato al seguente capitolo 4 verificherà con cadenza semestrale l'applicazione degli aggiornamenti e provvederà manualmente ad installarli laddove fosse necessario.
6. Viene distribuito un software antivirus aggiornato su tutte le postazioni. Esso è impostato in maniera da renderne automatico l'aggiornamento, con frequenza almeno settimanale. Laddove possibile, tale programma verrà impostato in maniera tale da non poter essere disattivato dall'utente. In ogni caso è fatto assoluto ed esplicito divieto agli utenti di manomettere o disattivare il software antivirus, pena la segnalazione del fatto per i provvedimenti disciplinari del caso laddove da tale comportamento non discendano più gravi conseguenze.
7. In mancanza di procedure di installazione automatiche, e comunque a titolo di verifica, con cadenza almeno semestrale, verrà effettuata una verifica ed un aggiornamento manuale del software antivirus su tutte le macchine. Un responsabile viene all'uopo nominato nel seguente capitolo 4.

3.3.3 Integrità e disponibilità dei dati

1. I dati che interessano più utenti sono inseriti in un sistema di directory sottoposte a backup. Ogni utente è abilitato ad entrare nelle directory di cui ha autorizzazione. Le autorizzazioni sono descritte nell'*allegato C*.
2. Il fileserver viene gestito internamente, le politiche di backup e di gestione della sicurezza e della disponibilità del fileserver vengono acquisite come allegato del presente DPS; in ogni caso devono garantire l'integrità dei dati con un salvataggio almeno settimanale, e la confidenzialità dei dati il cui ripristino deve poter avvenire solo sotto autorizzazione del Responsabile o del Titolare del Trattamento. La conservazione di tali backup deve avvenire secondo norme compatibili con quanto stabilito al punto 5 del paragrafo 3.2.
3. Il responsabile del trattamento individua inoltre altri volumi logici o aree di disco da sottoporre a backup sulle varie macchine, sulla base delle esigenze dell'Ente e di quanto determinato al punto 1. Per ogni volume, area di disco o base di dati viene chiaramente indicata la frequenza con cui il backup va effettuato, che in ogni caso sarà almeno settimanale. Tali

volumi e aree vengono registrati, insieme alle relative politiche di backup, nell'*allegato E*.

4. Sono nominati al successivo capitolo 4 uno o più incaricati del backup. Gli incaricati effettuano le seguenti operazioni:
   - Esecuzione dei backup come definito al punto precedente. Laddove possibile verranno implementate procedure automatiche.
   - Mantenimento di un elenco dei backup effettuati (mod. *PRI06 Registro backup* inserito tra gli allegati al DPS);
   - Archiviazione dei supporti secondo le disposizioni del presente documento;
   - Verifica, con cadenza almeno semestrale, della procedura di recovery dai supporti di backup e conseguentemente della leggibilità ed utilizzabilità del backup stesso.

3.3.4 Controllo degli accessi

1. Tutte le stazioni di lavoro che ospitano e trattano dati personali e/o sensibili debbono consentire l'accesso soltanto a persone opportunamente autenticate ed autorizzate.
2. Tutti gli applicativi disponibili in rete che consentono il trattamento di dati personali e/o sensibili debbono consentire l'accesso soltanto a persone opportunamente autenticate ed autorizzate.
3. L'autenticazione viene effettuata mediante un nome utente e una password
4. Il nome utente deve essere unico in tutta la rete aziendale, anche su macchine differenti, e non deve essere usato da persone diverse nemmeno in tempi diversi.
5. La password:
   - Non deve derivare dal nome utente o dai dati personali dell'utente;
   - Deve avere una lunghezza di almeno 8 caratteri (o la massima lunghezza possibile se inferiore a 8);
   - Non deve essere una semplice parola rintracciabile in un dizionario;
   - Deve contenere almeno un carattere non alfabetico, e/o un misto di lettere minuscole e maiuscole
6. Nome utente e password sono strettamente personali. L'utente è tenuto:
   - A non comunicare a terzi le password;
   - A non annotare le password su supporti posti in vicinanza della propria postazione di lavoro, o comunque incustoditi;
   - Ad attenersi a tutte le indicazioni contenute nel manuale per la sicurezza.
7. Vengono nominati uno o più amministratori di sistema
8. Il responsabile del trattamento fornisce agli amministratori di sistema i nominativi e la qualifica degli utenti autorizzati ad accedere agli applicativi disponibili in rete o ai server di rete, nonché i loro privilegi. Gli amministratori provvedono:
   - A definire, per ciascun utente, il nome utente e la password per il primo accesso;
   - A definire i gruppi necessari per rispettare i privilegi di utilizzo;
   - A consegnare agli interessati il nome utente e la password, unitamente a una copia del Manuale per la sicurezza.

9. Dove questo è tecnicamente possibile, gli Amministratori di Sistema impostano il sistema in modo da forzare l'utente:
   - A cambiare la propria password al momento del primo accesso;
   - A cambiare la password periodicamente, con una frequenza almeno trimestrale per i profili che trattano dati sensibili, ed almeno semestrale per gli altri.
   - A non poter riutilizzare la stessa password prima di quattro modifiche
10. Ad alcuni addetti può essere fornito dall'Ente un elaboratore personale (portatile o fisso) per uso esclusivamente aziendale.
11. Gli elaboratori di cui al punto 10 non vengono amministrati in modo centralizzato, ma sono sottoposti a tutte le normative di questo documento. In particolare:
   - L'utente si impegna a non disattivare il controllo antivirus
   - L'utente si impegna a rispettare i vincoli relativi all'uso e alla definizione di password e nome utente
   - L'utente si impegna a non installare sulla postazione software di provenienza illecita o non certa, e in generale qualsiasi software non preventivamente autorizzato dagli amministratori di sistema
12. Non appena venga meno la qualifica per cui l'elaboratore di cui al punto 10 è stato assegnato, esso deve essere immediatamente restituito, e deve essere verificata la possibilità di accedere a tutti i dati personali in esso contenuti. Tutte le password di accesso all'elaboratore devono essere cambiate nello stesso momento.
13. Gli amministratori di sistema provvedono, con cadenza almeno annuale, alla verifica degli elenchi degli utenti, e provvedono, previa verifica con il responsabile del trattamento, alla disattivazione delle utenze su cui risultasse qualche problema (mancato utilizzo da più di sei mesi, un elevato numero di tentativi di accesso non riusciti, o simili)
14. Gli interventi tecnici possono venire eseguiti solo dagli amministratori di sistema o da personale interno o esterno munito di autorizzazione scritta degli amministratori di sistema. Per tali interventi tecnici, qualsiasi password necessaria dovrebbe essere digitata dall'utente. Se ciò non fosse possibile, l'utente o il responsabile delle password può comunicarla all'incaricato della manutenzione: in tal caso essa dovrà essere cambiata dopo il termine dell'intervento di manutenzione e mai più riutilizzata su nessun sistema
15. Solo e soltanto nel caso in cui la conoscenza di una determinata password sia strettamente necessaria per poter accedere ad elenchi di dati in assenza dell'incaricato del trattamento, egli dovrà affidarne una copia, in busta chiusa, al Responsabile, che la custodirà sotto chiave. In caso di sostituzione della password, la nuova password andrà parimenti affidata con lo stesso meccanismo al Responsabile.

3.3.5 Autenticazione e profili

1. Il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato *profilo*, rispetto alle risorse del sistema informatico o dell'applicativo di trattamento in uso. Ciascun utente può appartenere ad uno o più profili.
2. Il responsabile del trattamento allo stesso modo informa gli amministratori di sistema delle eventuali variazioni ai privilegi necessarie per intervenuti mutamenti nel processo di trattamento affinché essi vengano tradotti in

pratica.

3.3.6 Trasmissione dei dati

1. Le connessioni telematiche si possono suddividere in 2 categorie:
   a) Connessioni provenienti dalla LAN, verso altre macchine della LAN;
   b) Connessioni provenienti dalla LAN verso Internet;
2. Le connessioni di tipo a) sono consentite, per finalità lavorative e nel rispetto delle norme del presente Documento. Nel caso vengano trasmessi o condivisi documenti contenenti dati personali, dovranno essere adottate misure opportune (condivisione mediante password) per verificare che l'accesso sia limitato a persone opportunamente autorizzate
3. Le connessioni di tipo b) sono consentite, mediante l'utilizzo del server proxy e del firewall come indicato dagli Amministratori di Sistema.
4. Ogni tipo di collegamento telematico non specificamente previsto è vietato.
5. In particolare sono vietate connessioni effettuate tramite modem da postazioni collegate alla rete dell'ufficio.
6. Il collegamento alla LAN di dispositivi quali PC portatili ed affini di proprietà dei dipendenti deve essere preventivamente autorizzato da un Amministratore di Sistema; il portatile deve essere configurato in maniera da corrispondere alla configurazione standard e ai requisiti del presente Documento.

3.3.7 Stampe di dati

1. Eventuali documenti stampati, contenenti informazioni di tipo personale o sensibile, vanno gestiti con le stesse procedure delineate per fascicoli e pratiche cartacee (paragrafo 3.2.5). Al termine del trattamento devono essere archiviati correttamente o distrutti in modo da renderne impossibile il recupero.
2. Le stampe di documenti contenenti informazioni sensibili devono essere effettuate su stampanti locali, o comunque sotto la diretta osservazione dell'utente.

3.3.8 Sistema di monitoraggio

1. Deve essere messo in atto un processo di controllo e verifica della sicurezza delle risorse hardware e software, attraverso l'utilizzo di appositi strumenti sia a livello di sistema informatico, sia in termini di gestione delle banche dati che in termini di applicazioni
2. Il sistema di controllo deve registrare:
   - Gli accessi alla rete e ai singoli elaboratori, riusciti e falliti
   - Gli accessi a banche dati e ad applicativi di rete, riusciti e falliti;
   - Gli accessi effettuati dalla rete Internet, o da qualsivoglia rete pubblica di telecomunicazioni, verso l'interno, con il massimo dettaglio possibile;
   - Gli eventuali rapporti dei sistemi antivirus.
3. Nessuno ha l'autorità per intervenire, modificare o bloccare i sistemi di controllo attivati, compresi i già menzionati software antivirus, tranne il Responsabile del Trattamento, con provvedimento scritto e motivato, per motivi di manutenzione o di aggiornamento del sistema di controllo stesso. In nessun caso i dati registrati dal sistema di controllo possono o

debbono essere corretti, modificati o cancellati.

4. Il responsabile del trattamento individua, tra gli amministratori di sistema, uno o più incaricati della verifica, almeno annuale, delle registrazioni di cui al precedente comma, e della loro archiviazione su supporto inalterabile.
5. L'individuazione delle responsabilità connesse a modifiche o letture non autorizzate di dati, o comunque l'individuazione di violazioni del presente documento programmatico e delle disposizioni impartite dal Responsabile del Trattamento o dagli Amministratori di Sistema, viene effettuata da uno degli Amministratori di Sistema esclusivamente su richiesta del Responsabile del Trattamento, oppure dietro ingiunzione dell'Autorità giudiziaria.
6. Fatta eccezione per quanto stabilito al punto precedente, gli archivi dei sistemi di controllo sono riservati e nessuno vi può accedere in nessun caso.

4 Distribuzione dei compiti e delle responsabilità

4.1 Identificazione del titolare del trattamento

Il *Titolare del Trattamento* è individuato per CONSORZIO ENFAPI TREVIGLIO nella persona del suo legale rappresentante.

4.2 Procedure per la nomina e la revoca degli incaricati

Il Titolare del Trattamento e/o il Consiglio d'Amministrazione nomina il *Responsabile del Trattamento* (mod. *PRI07 Nomina responsabile trattamento* inserito tra gli allegati al DPS).
Le figure elencate al successivo paragrafo 4.3 vengono nominate dal Responsabile del Trattamento. Esse possono essere revocate in qualsiasi momento mediante atto del Responsabile o degli organi direttivi. Gli incaricati possono richiedere di essere sollevati da tali mansioni. Tale richiesta sarà soddisfatta a discrezione del Responsabile, in base alle esigenze d'ufficio.

4.3 Elenco degli incaricati

Saranno nominati:

- Uno o più Amministratori di Sistema; se non nominato, coinciderà con il Responsabile del Trattamento (mod. *PRI08 Nomina incaricato ammin sistema* inserito tra gli allegati al DPS);
- Un responsabile per gli aggiornamenti del software, preferibilmente scelto tra gli amministratori di sistema (mod. *PRI08 …..*)
- Un responsabile per gli aggiornamenti degli antivirus, preferibilmente scelto tra gli amministratori di sistema (mod. *PRI08 …..*)
- Uno o più Incaricati del Backup, ciascuno con l'indicazione delle specifiche macchine o archivi per cui sono incaricati. Laddove non sia specificamente previsto un incaricato, gli Amministratori di Sistema sono implicitamente incaricati. (mod. *PRI08 … e* mod. *PRI11 Nomina incaricato interno amministraz.*)
- Un numero variabile di Incaricati del Trattamento, ognuno con specifici privilegi d'accesso determinati in base ai profili e ai trattamenti individuati al capitolo 1. (mod. *PRI09 Nomina incaricato contabilità* – mod. *PRI10 Nomina incaricato esterno amministraz* - mod. *PRI11 Nomina incaricato interno amministraz* - mod. *PRI13 Nomina incaricato interno esterno didattica* inseriti tra gli allegati al DPS*)*

Un elenco aggiornato degli incaricati sarà custodito in allegato a questo manuale (*allegato C*).
Per quanto riguarda gli incaricati al trattamento dei dati in forza presso il Consorzio Enfapi con contratto di lavoro a tempo indeterminato, la nomina si intende revocata alla data di cessazione del rapporto di lavoro oppure su indicazione del Responsabile del Trattamento: pertanto la nomina verrà redatta solo all'atto dell'assunzione del dipendente (si provvede a fornire la nomina ai lavoratori già in forza).
Per quanto riguarda invece tutti gli altri incaricati al trattamento dei dati in forza presso il Consorzio Enfapi con contratto di lavoro a progetto o come lavoratore autonomo libero professionista, la nomina si intende automaticamente revocata alla scadenza del contratto oppure su indicazione del Responsabile del Trattamento: pertanto, ad ogni inizio anno formativo, con la sottoscrizione del primo incarico si fornirà anche la nomina al trattamento dei dati (si provvede a fornire la nomina ai collaboratori già in forza).
Le nomine verranno archiviate nel fascicolo personale di ciascun addetto al trattamento dei dati e a fine anno archiviate con il curriculum vitae nel falcone costi comuni.

5 Interventi Formativi

5.1 Introduzione

A norma di legge gli Incaricati del Trattamento devono essere informati dei rischi individuati nel capitolo 2 e di come le relative contromisure, individuate nel capitolo 3, li possano ridurre. Questo, oltre ad essere un preciso requisito di legge, è anche un ragionevole principio: solo la formazione e la motivazione degli incaricati al trattamento dei dati personali e sensibili possono rendere efficaci le misure di sicurezza individuate.
Questo capitolo descrive le misure adottate per formare gli Incaricati.

5.2 Il manuale per la sicurezza ad uso degli incaricati

Il manuale per la sicurezza è lo strumento principale in uso agli incaricati al trattamento dei dati: viene adottato e aggiornato contestualmente al presente documento programmatico, e riassunte con termini chiari e limitatamente agli ambiti di interesse di ciascun incaricato, le seguenti informazioni:

- Panoramica delle disposizioni legislative in tema di tutela dei dati e criminalità informatica
- Analisi e spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema, interessato.
- Le misure di sicurezza adottate:
  - Misure di sicurezza fisiche da adottare;
  - Misure di sicurezza per la protezione dei sistemi informatici, prevenzione e contenimento del danno, strumenti di protezione hardware e software (in particolare antivirus e misure antiintrusione);
  - importanza e modalità di realizzazione delle operazioni di backup;

Il manuale per la sicurezza viene consegnato agli utenti contestualmente ai codici (nome utente e password) per l'accesso agli elaboratori elettronici (come risulta da Mod. *PRI14 Verbale interventi formativi* inserito tra gli allegati al DPS). Gli utenti hanno la responsabilità personale di leggere il manuale e di contattare un Amministratore di Sistema per chiedere delucidazioni sui comportamenti da tenere.

5.3 Altri metodi di formazione

Il responsabile del trattamento provvederà, anche per conto degli amministratori di sistema, a informare tempestivamente gli incaricati:

- della presenza di virus negli elaboratori;
- di prassi da parte del personale non conformi alle disposizioni di sicurezza;
- di altri eventi relativi alla sicurezza

Inoltre, il Titolare del Trattamento, eventualmente tramite il Responsabile, ove richiesto o ove se ne ravvisi la necessità, provvederà ad organizzare riunioni e corsi per l'illustrazione e la diffusione degli accorgimenti da adottare in tema di sicurezza.

6 Dati trattati all'esterno dell'Ente

6.1 Elenco dei trattamenti effettuati all'esterno dell'Ente

I dati personali e sensibili, trattati all'esterno dell'ente sono solamente quelli trasmessi allo Studio VERONELLI per l'elaborazione dei compensi e delle relative dichiarazioni fiscali previste dalla legge, e quelli trattati dal Rag. ROGNONI per le elaborazioni contabili e le relative dichiarazioni fiscali di legge..

7 Criteri di cifratura e gestione separata per i dati sensibili

Dalle risultanze esaminate, CONSORZIO ENFAPI TREVIGLIO non gestisce archivi di dati sensibili attinenti le disabilità fisiche, opinioni religiose o politiche, o dati relativi lo stato di salute o l'origine razziale ed etnica per cui sia richiesta la cifratura e/o la gestione in forma anonima.

Nel caso si rendesse necessario trattare questo tipo di dati, il Responsabile del Trattamento autorizzerà il trattamento, dando all'uopo le direttive tecniche necessarie per garantire il rispetto dei requisiti di legge.

8 Piano di verifica e revisione delle misure adottate

8.1 Introduzione

Le procedure contenute in questo documento si intendono valide e corrispondenti alla legge per quanto noto alla data della sua adozione.

Tuttavia è necessario:
- ❖ Accertare che le disposizioni del presente documento vengano effettivamente applicate (*verifica*)
- ❖ Aggiornare le disposizioni per adeguarsi ai cambiamenti imposti dall'evoluzione tecnologica, legislativa o dalle modifiche nei procedimenti amministrativi (*revisione*)

8.2 Verifica delle misure adottate.

8.2.1 Procedure generali di verifica

1. Le verifiche verranno svolte dal Responsabile del Trattamento o da un Amministratore di Sistema da lui incaricato.
2. Per ogni verifica sarà steso un accurato verbale (Mod. *PRI15 Verbale attività di controllo* inserito tra gli allegati al DPS), datato e firmato, conservato insieme al documento programmatico. Con cadenza annuale, in coincidenza con la revisione del Documento, tali verbali verranno riassunti, a cura del Responsabile del Trattamento, in un rapporto sull'applicazione del Documento Programmatico (Mod. *PRI16 Rapporto applicazione DPS* inserito tra gli allegati al DPS)
3. Eventuali mancanze, inadempienze, errori od omissioni a carattere personale andranno segnalate a cura del Responsabile del Trattamento ai responsabili per l'applicazione delle misure disciplinari previste dal contratto di lavoro.
4. Eventuali problemi di natura tecnologica dovranno essere risolti il più celermente possibile, compatibilmente con le esigenze tecniche e di bilancio. Il Responsabile del Trattamento è autorizzato a prendere le misure di emergenza necessarie per evitare danni.

8.2.2 Verifiche relative alla sicurezza fisica

1 Periodicamente sarà verificato, mediante controlli a campione, il rispetto delle misure di sicurezza fisica previste (chiusura delle serrature, inserimento degli allarmi, ecc.). Tali ispezioni dovranno essere tenute almeno una volta ogni sei mesi.

2 Periodicamente sarà verificato, mediante controlli a campione, il rispetto delle misure di sicurezza previste per il trattamento di documenti cartacei, in particolare il loro riposizionamento negli archivi e la chiusura di questi ultimi. Tali verifiche dovranno essere tenute almeno una volta ogni sei mesi.

3 Periodicamente, e dando un opportuno preavviso, dovranno essere verificati gli impianti rivelatori di incendio e gli impianti UPS, anche mediante prove pratiche. Tali ispezioni dovranno essere tenute

almeno una volta ogni sei mesi.

8.2.3 Verifiche relative alla sicurezza informatica

1 Periodicamente sarà verificata, mediante controlli a campione, l'esistenza e l'utilizzabilità delle copie di backup dei dati. Tali ispezioni dovranno essere tenute almeno una volta l'anno.

2 Periodicamente sarà verificata, mediante controlli a campione, l'installazione e la funzionalità dei software antivirus e il loro aggiornamento, nonché l'eventuale installazione di software non autorizzato sulle macchine. È data facoltà agli Amministratori di Sistema di intervenire immediatamente in caso di violazioni del Documento Programmatico per ripristinare la configurazione lecita delle macchine.

3 Gli amministratori di sistema provvedono, con cadenza almeno annuale, alla verifica degli elenchi degli utenti, e provvedono, previa verifica con il responsabile del trattamento, alla disattivazione delle utenze su cui risultasse qualche problema (mancato utilizzo da più di sei mesi, un elevato numero di tentativi di accesso non riusciti, o simili).

4 Periodicamente gli Amministratori di Sistema, o incaricati esterni, con l'assistenza di enti esterni, verificheranno la sicurezza perimetrale del sistema, controllando che non vi siano possibilità di accesso oltre a quelle specificamente consentite dal presente documento.

8.3 Revisione del presente documento

Il presente documento è da ritenersi accurato e rispondente ai termini di legge alla data dell'adozione. Successivamente, ogni anno, entro il 31 marzo, il Titolare del Trattamento, sentiti gli Amministratori di Sistema e tenendo in considerazione il rapporto sull'applicazione del documento stesso (mod. PRI16), ne emetterà una eventuale revisione che si considererà automaticamente adottata in sostituzione della precedente. La revisione interesserà il Documento Programmatico, tutti gli allegati e il Manuale per la Sicurezza.

La revisione sarà comunicata a tutti gli incaricati, distribuendo una informativa contenente le modifiche adottate e di loro diretto interesse. Nel caso di modifiche particolarmente estensive sarà distribuita una copia aggiornata del Manuale per la sicurezza.

Gli allegati e gli altri documenti di lavoro di seguito elencati possono essere aggiornati costantemente, al di fuori di questa procedura, dal Responsabile del Trattamento o dal Titolare.

8.3 Legge 231

Per le procedure relative alla Prevenzione dei reati informatici vedere anche:
1) Codice Etico dell'Ente,
2) MOG parte speciale E: reati informatici

ELENCO ALLEGATI e DOCUMENTI DI LAVORO

Allegato A Elenco delle chiavi e dei custodi e degli archivi

Allegato B Elenco dei software approvati

Allegato C e Cbis Elenco degli incaricati e dei profili di autorizzazione

Allegato D Elenco delle macchine

Allegato E Elenco delle aree e dei volumi logici sottoposti a backup

Allegato F Videosorveglianza

PRI01 Informativa CLIENTI_FORNITORI SENZA firma CONSENSO
PRI02 Informativa ALLIEVI CON firma CONSENSO
PRI03 Informativa RISORSE UMANE CON firma CONSENSO
~~PRI04 ELIMINATO~~
PRI05 Registro assegnazione chiavi
PRI06 Registro BACKUP e RECOVERING DATI SERVER – VERIFICA SW ANTIVIRUS e FILE DI MONITORAGGIO
PRI07 Nomina responsabile trattamento
PRI08 Nomina incaricato ammin sistema
PRI09 Nomina incaricato contabilità
PRI10 Nomina incaricato esterno amministraz
PRI11 Nomina incaricato interno amministraz
~~PRI12 ELIMINATO~~
PRI13 Nomina incaricato interno esterno didattica
PRI14 Verbale interventi formativi
PRI15 Verbale attività di controllo
PRI16 Rapporto applicazione DPS
PRI17 autorizzazioni accessi sistemi informatici
PRI18 autorizzazioni accessi al sistema dall'esterno (es. VPN, …)
PRI19 Relazione annuale verifica SW istallati nei computer del Centro con Validazione Direttore
PRI20 Validazione Presidente accessi banche date esterne della PA
PRI21 Ceck list: PARTE SPECIALE "E": REATI INFORMATICI