

DOCUMENTO

PROGRAMMATICO

SULLA SICUREZZA



ANNO DI RIFERIMENTO
2010

UNIVERSITÀ TELEMATICA PEGASO
VIA VITTORIA COLONNA, 14 – 80121 NAPOLI
CODICE FISCALE 05411471211

INDICE

- 1. Dati Aziendali**
- 2. Regola 19.1 – Elenco dei Trattamenti**
- 3. Regola 19.2 – Competenze**
- 4. Regola 19.3 – Analisi dei Rischi**
- 5. Regola 19.4.1 – Misure di Sicurezza Adottate**
- 6. Regola 19.4.2 – Scheda Descrittiva delle Misure di Sicurezza adottate**
- 7. Regola 19.5 – Criteri e Procedure**
- 8. Regola 19.6 – Formazione**
- 9. Regola 19.7 – Trattamenti affidati all'esterno**

Allegati:

- 1. allegato 1 - Planimetria descrittiva**
- 2. allegato 2 - lettera nomina responsabile del trattamento**
- 3. allegato 4 - lettera nomina incaricati al trattamento e Regolamento di sicurezza**
- 4. allegato 5 - Organigramma**

GENERALE

Dati Aziendali

Descrizione Documento

Il presente **Documento Programmatico sulla Sicurezza** è redatto, ai sensi degli articoli 33 e seguenti del D.Lgs. 196/2003 e secondo le previsioni dell'Allegato 2 a tale decreto, per definire e descrivere le politiche di sicurezza adottate dall'Ateneo in materia di trattamento di dati personali ed i criteri organizzativi seguiti per la loro attuazione e per fornire idonee informazioni a riguardo anche a parti terze.

Dati Riguardanti il Titolare del Trattamento

Titolare del Trattamento:
Università Telematica Pegaso

Codice Fiscale 05411471211

SEDE LEGALE - Indirizzo: Via Vittoria Colonna, 14
Città: NAPOLI
CAP: 80121

UNITA' LOCALE 1 - Indirizzo: Via San Vincenzo Lotto12
Città: Mercato San Severino (SA)
CAP: 84085

PRESIDENTE DEL COMITATO ESECUTIVO:

- **DANILO IERVOLINO NATO A NAPOLI IL 02/04/1978**
RESIDENTE IN PALMA CAMPANIA ALLA VIA TRIESTE, 104
CAP 80036
Codice Fiscale: RVLN78D02F839W

GENERALE

*Dati Aziendali
(...segue...)*

Dati Riguardanti i Responsabili del Trattamento

SEDE LEGALE: Via Vittoria Colonna, 14
80121 NAPOLI

Nominativo: Dott. Francesco Accardo

Indirizzo: Parco San Paolo 16

Città: NAPOLI

CAP: 80126

Codice Fiscale: CCRFNC77P15F839B

UNITA' LOCALE 1 - San Vincenzo Lotto12
84085 MERCATO SAN SEVERINO (SA)

Nominativo: Dott. Francesco Accardo

Indirizzo: Parco San Paolo 16

Città: NAPOLI

CAP: 80126

Codice Fiscale: CCRFNC77P15F839B

Tipologia dei Dati Trattati

- Dati Personali (**DP**)
- Dati Sensibili (**DS**)

Regola 19.1

Elenco dei Trattamenti

INFORMAZIONI ESSENZIALI

Le informazioni fornite di seguito sono valutate utile supporto per fornire informazioni idonee a valutare la politica di sicurezza perseguita dall'Ateneo.

La Università telematica Pegaso effettua il Trattamento dei Dati Personali su documentazione cartacea e mediante la strumentazione elettronica hardware presente presso la sede e le unità locali.

Delle modalità di trattamento e conservazione della documentazione cartacea ed elettronica dei dati, nonché della specifica descrizione della tipologia e dell'ubicazione fisica delle macchine hardware inventariate si darà descrizione in altra parte del presente Documento Programmatico sulla Sicurezza (DPS).

E' stata individuata n. 1 (una) Figura di Responsabilità nell'Organizzazione, così come desumibile dall'Organigramma allegato, a valere sia per la Sede Legale in Napoli e che per l'Unità Locale di Mercato San Severino (SA).

Il dott. Francesco Accardo è stato nominato **RESPONSABILE DEL TRATTAMENTO**, per la **SEDE LEGALE in Napoli** e per l'**UNITA' LOCALE di Mercato San Severino (SA)**.

Egli, nella sua qualità di Responsabile del trattamento è individuato come soggetto referente delle diverse figure dell'organizzazione per la determinazione, la pianificazione e l'implementazione delle procedure organizzative necessarie al trattamento ed alla tutela dei dati personali.

In via assolutamente generale e salvo quanto meglio specificato in altra parte del presente DPS, a livello di linee guida, l'esigenza di tutela dei dati trattati all'interno dell'Ateneo si è concentrata sulle seguenti aree di intervento:

1. **Accesso ad Internet**
2. **Installazione di Software non attinenti allo svolgimento della attività dell'Ateneo**
3. **Utilizzo di Supporti rimovibili sulle postazioni Client**
4. **Telefonate dalla sede verso l'esterno**
5. **Gestione documentazione Cartacea**

definendo le seguenti **linee guida**, di cui si è provveduto a diffondere il contenuto con chiarezza e dettaglio presso le sedi di lavoro, con precisa indicazione della possibilità di effettuare controlli graduali a campione per richiamare l'Organizzazione (reparti, uffici e gruppi) all'osservanza del regolamento interno.

(...continua...)

- **Accesso ad Internet**: considerata la pericolosità del canale telematico, ai fini della tutela dei Dati Trattati, **presso la sede di Napoli** si è deciso di inibire la navigazione in Internet su tutte le macchine hardware Client che accedono al Server, consentendo, su quelle non connesse al Server, per default esclusivamente la navigazione su siti Istituzionali necessari allo svolgimento dell'attività. Eventuali richieste di accesso a siti Internet diversi da quelli già autorizzati dal Responsabile del Trattamento, dovranno essere a Lui presentate dai singoli soggetti interessati. Effettuata una verifica della necessità di consultare la specifica pagina web e della sicurezza del sito Internet, il Responsabile del Trattamento provvederà ad autorizzarne, anche temporaneamente, l'accesso. Copia delle richieste di accesso con indicazione del soggetto da cui provengono, è conservata anche in modalità digitale, agli atti dell'Ateneo. **Presso la sede di Mercato San Severino (SA)**, invece, si precisa che su tutte le macchine hardware è consentita esclusivamente la navigazione in Internet su siti Istituzionali necessari allo svolgimento dell'attività, ma che non è stata inibita la navigazione su altri siti. Si precisa che sono effettuati controlli a campione relativamente alla navigazione Internet. Si precisa, che il controllo graduale potrà avvenire solo nel caso in cui si siano presentate delle ripetute anomalie.
- **Installazione di Software non attinenti allo svolgimento della attività dell'Ateneo e/o Utilizzo di Supporti rimovibili sulle postazioni Client**: **presso la sede di Napoli**, per default sono state disattivate tutte le periferiche native della macchine hardware Client che accedono al Server (CD, DVD etc) e tutte le porte di connessione di unità rimovibili esterne (porte seriali o USB). **Presso la sede di Mercato San Severino (SA)**, invece, pur non avendo disattivato tutte le periferiche native e le porte di connessione, gli utenti dispongono di accessi non privilegiati (utente limitato). Pertanto per entrambe le Unità locali, eventuali richieste di installazione software dovranno essere presentate ai rispettivi Responsabili del Trattamento dai singoli soggetti interessati.

(...continua...)

Effettuata una verifica della necessità di installazione, **presso la sede di Napoli**, il Responsabile provvederà ad autorizzarla mediante attivazione, anche temporanea, della periferica o della porta di connessione, mentre **per la Unità di Mercato San Severino (SA)**, il Responsabile personalmente eseguirà le installazioni richieste.

Copia delle richieste di installazione con indicazione del soggetto da cui provengono, è conservata anche in modalità digitale, agli atti dell'Ateneo.

- **Telefonate dalla sede verso l'esterno**: la politica perseguita è quella della limitazione delle stesse laddove non strettamente necessarie allo svolgimento delle attività dell'Ateneo. In caso di necessità, i soggetti autorizzati ad effettuare chiamate verso l'esterno, comunicano il numero di telefono ai Responsabili che provvedono ad inserirlo in Database autorizzativo.

In particolar modo viene qui fatta rilevare la necessità di tutela del trattamento dei recapiti telefonici forniti dai soggetti interessati ad esser ricontattati a seguito di una loro telefonata al Call Center che risponde al numero 800.911.771. Particolari metodologie di acquisizione del consenso da parte degli studenti interessati ad esser ricontattati sono state implementate e saranno descritte alla **Regola 19.1 pagina 9** del presente DPS.

Presso la unità locale di Mercato San Severino (SA), i soggetti che necessitano di effettuare telefonate, compilano personalmente un registro di chiamate in uscita, con indicazione del numero chiamato e della motivazione. Il registro è detenuto presso la sede.

I Responsabili del trattamento periodicamente e senza preavviso, provvedono ad una analisi a campione delle telefonate effettuate non riconducibile al soggetto che le ha effettuate, richiedendo delucidazioni all'Organizzazione (Reparti, Uffici o Gruppi di Lavoro) in merito alla sopravvenuta necessità od all'evenienza già riscontrata.

Tali controlli, se necessari, verranno svolti con assoluto rispetto degli operatori interessati.

(...continua...)

- **Gestione della documentazione cartacea:** la documentazione cartacea è conservata in armadi chiusi a chiave ad ante non trasparenti presenti in stanza chiusa a chiave degli Uffici. Le chiavi di accesso alla stanza ed agli armadi è in possesso dei soli Responsabili del Trattamento che provvedono a seguire personalmente agli accessi richiesti. La documentazione non più utile, laddove contenga dati personali è cestinata previa sua distruzione con “*distruggi-documenti*” presente in sede.

Nominativo: Francesco Accardo (*riferisce ad Amministratore Delegato*)

Ruolo: Responsabile del trattamento dell’Unità Locale di Napoli

Tipo di Attività Svolta: Amministrazione di sistema informatico

Soggetti a lui referenti: Dipendenti

Tipologia dei Dati Tutelati: **TUTTI** (*ad eccezione dei dati contabili*) ed in particolare:

DP – Nominativo – Indirizzo di Residenza – Codice Fiscale -
Recapiti Telefonici e Telematici degli Studenti e degli ECP

DS – *Curricula studiorum* - Percorsi Formativi - Carriera Accademica
Dati sensibili relativi al personale dipendente – Conservazione delle
Password degli incaricati – Violazioni al Regolamento interno

Tipologia degli Archivi: Archivi Informatici e Cartacei

Luogo fisico di Conservazione: Server – Archivi Cartacei

Strumentazione Elettronica su cui interviene: Server / Client

Trasmissione ad altri soggetti: **NO**

Accessi Hardware: **TUTTI**

Accessi Software: **TUTTI**

Accesso ad Internet: **Illimitato**

Procedure di Backup: **SI**

(...continua...)

A seguire saranno descritte le diverse aree organizzative analizzandole avendo a riguardo le Figure di Responsabilità e descrivendo, per ognuna di esse, il Tipo di Attività svolta, i soggetti Interessati e la tipologia di dati trattati.

Preliminarmente si intende analizzare quale sia la fonte dei dati personali dei potenziali studenti analizzandola sotto il profilo su indicato.

Unità di Napoli

Call Center

È stato istituito il numero verde gratuito 800.911.771, riportato anche nelle iniziative pubblicitarie, al fine di consentire ai soggetti interessati, il contatto con l'Università.

In particolare, e soprattutto per le finalità di cui al D.Lgs. 196/2003, è richiesta ai soggetti che intendono ricevere informazioni relativamente ai corsi di studio una esplicita manifestazione di consenso.

Dal momento che il primo contatto avviene ad opera del soggetto interessato, la procedura definita consiste nel richiedere i dati anagrafici ai soggetti che contattano il call center per poi trasferire i nominativi all'Ufficio Commerciale che si preoccuperà di fornire la necessaria assistenza. In fase di primo contatto, pertanto, gli operatori del Call Center richiedono i Dati anagrafici ed i recapiti telefonici al soggetto interessato registrando su supporto digitale la manifestazione di consenso e la manifestazione di volontà di esser ricontattati. Tale manifestazione di consenso è conservata fino al momento della eventuale iscrizione, laddove è sostituita dal consenso scritto necessario ai fini dell'immatricolazione.

Il Responsabile della Sicurezza dell'Unità di Napoli si preoccupa dello smaltimento dei consensi digitali non più necessari per sostituzione con consensi per iscritto.

Eventuali dinieghi al trattamento dei dati precedentemente acconsentito vanno comunicati per iscritto al Responsabile per la Sicurezza presente in sede a Napoli.

Tipo di Attività Svolta: Call Center / Record consensi telefonici

Luogo di svolgimento: Unità di Via Vittoria Colonna 14

Soggetti Interessati: Studenti

Tipologia dei Dati Trattati:

DP – Nominativi ed Indirizzi e recapiti telefonici

Note: I dati anagrafici sono richiesti per agevolare il contatto da parte dell'Ufficio Commerciale. Il consenso al trattamento dei dati forniti è registrato in forma digitale e conservato su Server

Luogo fisico di Conservazione: Sede

Trasmissione ad altri soggetti: SI, dell'Organizzazione

(...continua...)

I dati ottenuti attraverso il consenso telefonico e quelli poi confermati con il consenso per iscritto sono trattati da diverse figure nell'ambito dell'organizzazione.

Sono stati individuati i seguenti n. 3 (tre) soggetti responsabili:

Direttore Amministrativo

Dott. Gian Giuseppe Pecorella – riferisce a Amministratore Delegato

La Direzione Amministrativa dell'Ateneo è affidata al Dottor Gian Giuseppe Pecorella, Dottore Commercialista con studio in Napoli alla Via Kerbaker, 91.

In qualità di Direttore Amministrativo, il Dottor Gian Giuseppe Pecorella tratta dati personali ed anagrafici tanto degli studenti ed ECP che di Clienti e Fornitori in generale.

La tenuta della contabilità dell'Ateneo ed il deposito delle scritture contabili è affidato alla **Seconta Sas con sede di Napoli alla Via Kerbaker 91**, CED esterno.

I dati della contabilità e la documentazione correlata, trattati presso il CED esterno su software di cui lo stesso CED è licenziatario, sono consultabili attraverso Internet dalla sede di Via Vittoria Colonna, 14. È altresì eseguita presso il CED esterno, la scansione dei documenti analogici in formato digitale.

In particolare, attraverso una funzionalità propria del software di contabilità e mediante una installazione Client dello stesso presso l'unità locale di Napoli, è possibile l'accesso alla contabilità ed alla documentazione correlata in remoto.

Il CED provvede, periodicamente alla Stampa della Documentazione derivante dalla tenuta della Contabilità (Iscrizioni, Quietanze etc) inviandola all'Ateneo presso la sede di Napoli.

Dalla postazione in utilizzo al Dott. Pecorella, è possibile l'accesso ad Internet che per la posizione ricoperta dal Professionista nell'organizzazione, è illimitato.

Altresì illimitata è la possibilità di effettuare telefonate inerenti allo svolgimento della propria attività nell'organizzazione.

Sotto le sue direttive, tanto il CED Esterno, quanto il Personale Amministrativo dell'Ateneo, eseguono le proprie attività ed organizzano il monitoraggio dello stato di avanzamento delle pratiche di iscrizione, sollecitando l'invio della documentazione eventualmente mancante ed la fase relativa alla gestione del credito.

(...continua...)

Tipo di Attività Svolta: Tenuta della Contabilità, Archivi nominativi e corrispondenza da e verso tali soggetti

Luogo di svolgimento: Sede dell'Ateneo Napoli e CED Esterno

Soggetti Interessati: Studenti/ECP - Clienti / Fornitori

Tipologia dei Dati Trattati:

DP – Nominativi ed Indirizzi

DS – Dati personali

Note: I dati anagrafici vengono gestiti per la tenuta della contabilità generale e per la gestione degli adempimenti civili e fiscali correlati

Luogo fisico di Conservazione: Sede di Napoli e CED Esterno

Trasmissione ad altri soggetti: NO - EVENTUALE

NOTE: I dati anagrafici e contabili, attraverso una funzionalità del software gestionale **MEXAL** in uso presso il CED Esterno, possono essere consultati dall'Ufficio del Consulente Amministrativo. La documentazione correlata e scansionata presso il CED esterno od in sede è visibile mediante gestionale documentale **ARXivar**, di cui il CED è licenziatario, per una cui descrizione si rinvia alla pagina 16.

Tipo di Attività Svolta: Gestione Dati Relativi alla Carriera Scolastica

Soggetti Interessati: Studenti

Tipologia dei Dati Trattati:

DP – Dati relativi alla Carriera Scolastica

DS - Dati relativi alla Carriera Scolastica

Luogo fisico di Conservazione: Strumentazione Elettronica dello Studio Professionale / Archivi Cartacei presso la sede di Napoli

Trasmissione ad altri soggetti: NO

NOTE: La procedura di immatricolazione degli studenti prevede che, effettuato il pagamento, essi facciano pervenire documentazione relativa alla propria carriera scolastica, oltre che documentazione di tipo anagrafico presso la sede dell'Ateneo. Accertata la regolarità della documentazione pervenuta, la documentazione scansionata è conservata elettronicamente sul database del CED Esterno e/o su quello dell'Ateneo, quella cartacea è conservata presso la sede in Area chiusa a chiave ed i dati relativi all'immatricolando studente vengono trattati per l'attribuzione del numero di matricola e poi gestiti presso la sede dell'Ateneo che provvede all'attribuzione delle passwords di accesso alla piattaforma formativa gestita presso la sede di Mercato San Severino. Le passwords di accesso alla piattaforma formativa non sono note al Responsabile né agli Incaricati della sede di Napoli, né a quelli di Mercato San Severino (SA).

Le passwords attribuite sono comunque modificabili liberamente dagli Studenti in fase di Primo Accesso alla Piattaforma didattica.

Il Ced Esterno cui si è fatto riferimento e che collabora nei modi anzidetti, detenendo temporaneamente o continuativamente Documentazione e Dati del cui trattamento è Titolare l'Ateneo è:

- **Seconta di Marco Magri & C. Sas**

Via KERBAKER 91- Piano Terra – 80128 NAPOLI
C.F. e P.IVA 05463671213

A tale soggetto esterno è stata richiesta ed è stata resa apposita dichiarazione scritta in cui viene certificata la conformità del proprio sistema informativo e della propria struttura alle previsioni della normativa sulla privacy. Tale dichiarazione è conservata agli atti dell'Ateneo.

(...continua...)

Vice Amministratore di Sistema

Sig. Mauro Giuseppe – riferisce a Responsabile Sicurezza /

riferisce a Direttore Amministrativo

Collaboratori: Loredana Livigni – Ufficio Commerciale

Nella sua qualità di Vice Amministratore di Sistema, il Sig. Mauro Giuseppe ha l'accesso a tutti i dati personali già descritti relativamente all'Amministratore di sistema Dott. Francesco Accardo, e può operare esclusivamente in caso di assenza od impedimento del Dott. Francesco Accardo e dietro specifica autorizzazione di quest'ultimo, relazionando per iscritto allo stesso sulle attività svolte o sulle iniziative intraprese in vece di Vice Amministratore.

Nell'esercizio delle sue mansioni ed in collaborazione con la dipendente Loredana Livigni, egli riceve i recapiti telefonici dei soggetti che, chiamato in numero verde, hanno rilasciato i propri recapiti ed il consenso ad essere ricontattati.

Non è consentito al Sig. Mauro né alla Sig. Livigni, contattare autonomamente soggetti che non abbiamo precedentemente rilasciato il consenso al trattamento dei propri dati personali.

La loro mansione consiste nello svolgere una funzione di orientamento ai potenziali studenti interessati.

Tipo di Attività Svolta: Attività Commerciale e di Orientamento

Luogo di svolgimento: Unità locale di Via Vittoria Colonna 14

Soggetti Interessati: Studenti

Tipologia dei Dati Trattati:

DP – Nominativi, indirizzi e recapiti telefonici

Note: L'Università ha predisposto un numero verde gratuito al quale i soggetti interessati ai servizi formativi offerti possono telefonare in ogni momento della giornata. La procedura è quella secondo cui tali soggetti, se interessati, vengano richiamati dai responsabili commerciali e per tale motivo è necessario che essi comunichino i propri dati personali al Call Center. La necessità di doverli richiamare comporta la necessità che essi acconsentano al trattamento ed all'utilizzo dei dati rilasciati. La procedura adottata consiste nella registrazione, previamente comunicata al soggetto, della telefonata nella parte in cui il soggetto che ha contattato il Call Center rilascia i propri dati anagrafici e nella parte in cui gli viene chiesta l'autorizzazione al trattamento dei dati personali, includendo la risposta del soggetto autorizzante.

Luogo di Conservazione: i file relativi ai consensi sono conservati su Server

Tipologia degli Archivi: Archivi Informatici

Trasmissione ad altri soggetti: SI, Unità Locale di Salerno

Accesso ad Internet: Limitato

Procedure di Backup: NO

Telefonate in uscita autorizzate: solo se ricevuto il consenso.

(...continua...)

Responsabile ECP

Dott. Mario Palmiero – riferisce a Consulente Amministrativo

Da un punto di vista organizzativo, ai fini del raggiungimento dei fini istituzionali volti alla diffusione, alla facilitazione all'accesso allo studio ed all'orientamento alla formazione universitaria e post universitaria, l'Ateneo ha delegato parte delle proprie attività a soggetti esterni autonomi, denominati ECP (E-Learning Center Point), per una cui elencazione si rinvia ad apposita sezione del sito www.unipegaso.it.

L'ECP è una entità autonoma ed indipendente, selezionata dall'Ateneo, che si configura come una propagazione tecnica ed organizzativa dell'Ateneo attraverso la quale, gli studenti, utilizzando l'organizzazione propria dell'ECP, possono utilizzare le strutture messe a loro disposizione per seguire in via telematica il percorso formativo prescelto. L'ECP inoltre assiste lo studente nelle scelte di studio e nell'eventuale disbrigo delle pratiche amministrative.

Esso va configurato come collaboratore esterno dal momento che, detenendo parte di dati di cui è Titolare l'Università, ad esso è richiesta in fase contrattuale una dichiarazione di conformità dei propri sistemi informativi e delle proprie strutture alle prescrizioni in materia di privacy, oltre ad essergli stato esplicitamente comunicato di non utilizzare i dati per finalità diverse da quelle per cui ne viene in contatto.

Il responsabile ECP ed i propri collaboratori studiano la necessità di intraprendere nuove partnerships ECP e pertanto sono autorizzati alla navigazione su computer stand-alone non connesso a Server senza limiti ed alla consultazione di dati su periferiche esterne.

Data la sua posizione nell'organizzazione, potrà trattare i dati degli studenti provenienti dall'attività degli ECP, secondo le politiche perseguite dall'Ateneo.

Giustificcherà comunque per iscritto le proprie attività che comportano il Trattamento di dati personali.

Tipo di Attività Svolta: gestione ECP

Luogo di svolgimento: Unità locale di Via Vittoria Colonna 14

Soggetti Interessati: ECP – soggetti esterni

Tipologia dei Dati Trattati:

DP – Nominativi, indirizzi e recapiti telefonici

Luogo di Conservazione: Client Stand - alone

Tipologia degli Archivi: Archivi Informatici e Cartacei

Trasmissione ad altri soggetti: NO

Accesso ad Internet: Illimitato con report

Procedure di Backup: NO

Telefonate in uscita autorizzate: Tutte con report

(...continua...)

Unità di Salerno

Nominativo: Accardo Francesco

Ruolo: Responsabile del trattamento dell'Unità Locale di Mercato San Severino (SA).

Soggetti a lui referenti: Dipendenti

Tipologia dei Dati Tutelati: **TUTTI** (*ad eccezione dei dati contabili*) ed in particolare:

DP – Nominativo – Indirizzo di Residenza – Codice Fiscale -
Recapiti Telefonici e Telematici degli Studenti

DS – *Curricula studiorum* - Percorsi Formativi - Carriera Accademica
Dati sensibili relativi al personale dipendente – Conservazione
delle Password degli incaricati – Violazioni al Regolamento
interno

Tipologia degli Archivi: Archivi Informatici e Cartacei

Luogo fisico di Conservazione: Server – Archivi Cartacei

Strumentazione Elettronica su cui interviene: Server / Client

Trasmissione ad altri soggetti: **NO**

Accessi Hardware: **TUTTI**

Accessi Software: **TUTTI**

Accesso ad Internet: **Illimitato**

Procedure di Backup: **SI**

Operatori informatici ed archivisti

— riferiscono a Responsabile del trattamento (Dott. Francesco Accardo)

Gli operatori informatici e gli archivisti hanno l'accesso a tutti i dati personali relativi agli studenti immatricolati iscritti ai corsi di studio. In particolare, ricevono ed utilizzano i recapiti telefonici per la gestione del loro percorso formativo.

In occasione delle procedure di iscrizione, attribuiscono allo studente le password di accesso alla piattaforma didattica, attraverso la quale lo stesso potrà seguire i corsi e visualizzare la propria posizione.

Non è consentito agli operatori informatici, contattare autonomamente soggetti che non siano iscritti.

Tipo di Attività Svolta: Attività amministrativa

Luogo di svolgimento: Unità locale di San Vincenzo lotto 12
Mercato San severino (SA)

Soggetti Interessati: Studenti

Tipologia dei Dati Trattati:

DP – Nominativi, indirizzi e recapiti telefonici

Luogo di Conservazione: Pc

Tipologia degli Archivi: Archivi Informatici e cartacei

Trasmissione ad altri soggetti: **eventuale (a Napoli)**

Accesso ad Internet: **Limitato alla ricerca**

Procedure di Backup: **SI**

Telefonate in uscita autorizzate: solo se ricevuto il consenso dallo studente

Unità di Salerno

Nominativo: Giuseppe De Simone

Ruolo: Responsabile del trattamento dell'Unità Locale di Mercato San Severino (SA).

Tipologia dei Dati Tutelati: **TUTTI** (*ad eccezione dei dati contabili*) ed in particolare:

DP – Nominativo – Indirizzo di Residenza – Codice Fiscale -
Recapiti Telefonici e Telematici degli Studenti

DS – *Curricula studiorum* - Percorsi Formativi - Carriera Accademica
Conservazione delle Password degli incaricati – Violazioni al
Regolamento interno

Tipologia degli Archivi: Archivi Informatici e Cartacei

Luogo fisico di Conservazione: Server – Archivi Cartacei

Strumentazione Elettronica su cui interviene: Server / Client

Trasmissione ad altri soggetti: **NO**

Accessi Hardware: **TUTTI**

Accessi Software: **TUTTI**

Accesso ad Internet: **Illimitato**

Procedure di Backup: **SI**

Nucleo di Valutazione

Nominativo: Giuseppe De Simone

Ruolo: Referente Nucleo di Valutazione

Tipologia dei Dati Tutelati: **TUTTI** (*ad eccezione dei dati contabili*) ed in particolare:

DP – Nominativo – Indirizzo di Residenza – Codice Fiscale -
Recapiti Telefonici e Telematici degli Studenti

DS – *Curricula studiorum* - Percorsi Formativi - Carriera Accademica

Tipologia degli Archivi: Archivi Cartacei

Luogo fisico di Conservazione: Archivi Cartacei

Strumentazione Elettronica su cui interviene: PC

Trasmissione ad altri soggetti: **NO**

NOTE: Gli studenti interessati all'iscrizione ai corsi formativi dell'Ateneo, inviano la documentazione necessaria alla Unipegaso Spa che ne verifica la correttezza formale e sostanziale.

Per l'attribuzione di eventuali Crediti Formativi la Unipegaso Spa trasmette al Nucleo di Valutazione copia della documentazione ricevuta e relativa al Curriculum Studiorum dell'immatricolando studente in formato elettronico.

Il soggetto, analizzata la documentazione dopo averla stampata, la in armadi chiusi a chiave presso la Unità Locale di Mercato San Severino (SA), distruggendo quella irrilevante ai propri fini mediante "*distruggi- documenti*".

Operatori informatici e Tutor

I soggetti operanti presso la sede di Salerno, ricoprono le seguenti mansioni:

- **Docenti;**
- **Tutor Metodologici**
- **Tutor Disciplinari;**
- **Coordinatori Didattici e Post Laurea.**

Essi hanno l'accesso ai dati personali relativi agli studenti immatricolati iscritti ai corsi di studio.

In particolare, i **Docenti** sono detentori solo temporanei della documentazione relativa alle sedute d'esame dal momento che al termine di ogni seduta d'esame la consegnano presso la sede Legale dell'Ateneo in Napoli.

I Tutor, utilizzano i recapiti telefonici ed email degli studenti per la gestione del percorso formativo essendo individuati dall'Ateneo come incaricati alla risoluzione delle diverse problematiche degli studenti tanto in termini tecnici legati all'utilizzo della piattaforma formativa quanto in termini didattici in senso stretto ed avendo la necessità di rispondere ai quesiti posti dagli Studenti stessi.

In particolare, successivamente all'iscrizione e dopo la consegna delle Password, effettuano il monitoraggio delle connessioni alla piattaforma didattica, necessario per la certezza della frequenza dei corsi ed eventualmente in caso di mancati accessi, contattano direttamente gli studenti per comprenderne i motivi e fornire assistenza.

Non è consentito agli operatori informatici nè ai Tutor, contattare autonomamente soggetti che non siano iscritti.

I Coordinatori Didattici e Post Laurea non utilizzano i Dati degli studenti essendo esclusivamente soggetti dell'Organizzazione di Ateneo.

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

(continua)

Alla data di redazione del presente documento, risultano **n. 41 (quarantuno) prestatori di Lavoro dipendente**

DIPENDENTI SEDE NAPOLI			
COGNOME/NOME	MATRICOLA	CODICE FISCALE	DATA ASSUNZIONE
BONAZZA VINCENZO	000012	BNZVCN69L21D548O	06/01/2008
BOSSA AZZURRA	000051	BSSZRR86E67F839D	01/05/2010
CASANOVA DANIELE	000055	CSNDNL63L15L259Z	19/01/2010
CASSIANI INGONI LUNA	000027	CSSLNU72B41F839B	03/02/2009
CIVITILLO DANIELA	000028	CVTDNL80P49F839N	03/02/2009
DE GAETANO PATRIZIO	000030	DGTPRC65A15G902M	03/06/2009
D'ELIA FRANCESCA	000056	DLEFNC82T49F924V	19/01/2010
DI DONATO FLORA	000058	DDNFLR71E44A489E	19/01/2010
DONATI MARIA	000016	DNTMRA73D65F839S	25/09/2008
ENNA ROMINA	000060	NNERMN68E53H703J	02/01/2010
FRAGNITO RICCARDO	000005	FRGRCR47D16C557E	10/01/2007
LA VECCHIA LOREDANA	000061	LVCLDN65B48I058H	02/01/2010
LIVIGNI LOREDANA	000054	LVGLDN78B43C495K	01/05/2010
MARTINIELLO LUCIA	000011	MRTLUC69R69F230C	06/01/2008
MAURO GIUSEPPE	000047	MRAGPP73P29G964S	01/05/2010
MUROLO MASSIMILIANO	000029	MRLMSM72M30F839I	03/06/2009
PALMIERO MARIO	000053	PLMMRA76D02F839F	01/05/2010
SACCONI GIUSEPPE	000057	SCCGPP64P17E456M	19/01/2010
SANSONE ANTONIETTA	000007	SNSNNT61R68F839E	25/09/2007
VETRANO RAFFAELA	000042	VTRRFL73C64B565V	12/11/2009

DIPENDENTI SEDE MERCATO SAN SEVERINO			
COGNOME/NOME	MATRICOLA	CODICE FISCALE	DATA ASSUNZIONE
ANNARUMMA CARMELA	000021	NNRCML74S53L845I	11/01/2008
BOTTA ANTONELLA	000049	BTTNNL77C57H703D	01/05/2010
CILIENTO EMANUELA	000043	CLNMNL83L48H703D	01/05/2010
COSCIA FRANCESCO SALVATORE	000059	CSCFNC60A01A228T	26/01/2010
COZZARELLI CARLA	000035	CZZCRL72H54H703Z	10/01/2009
D'AMICO ALESSANDRO	000032	DMCLSN85E31H703X	20/05/2009
DE SIO ALESSANDRA	000022	DSELSN73P54H431W	11/01/2008
DI GENNARO PELLEGRINO	000044	DGNPLG84C17A509I	01/05/2010
FALCO FILOMENA	000045	FLCFMN76H45F912Y	01/05/2010
FEOLA ELVIA ILARIA	000036	FLELLR81E71A509F	10/01/2009
FERRARO BRIGIDA	000037	FRRBGD80E64I234V	10/01/2009
FRAGNITO ANNACLAUDIA	000038	FRGNCL83E64A509Y	10/01/2009
IANNONE ANNA	000048	NNNNNA63H41F138W	01/05/2010
IANNACCONE SIMONA	000040	NNCSMN78A68A509Q	10/01/2009
MATARAZZO MODESTINO	000046	MTRMST83M28A509B	01/05/2010
ROMANO CARLO	000033	RMNCRL81T06C933N	17/06/2009
SALZILLO SALVATORE	000050	SLZSVT80R23B963I	01/05/2010
SORRENTINO CLORINDA	000039	SRRCRN82L62A509A	10/01/2009
TEDESCO INES	000023	TDSNSI81C42I234R	11/01/2008
VIVONA ANGELINA	000009	VVNNLN75C44A773W	11/02/2007
ZAMMARRELLI FRANCESCA	000025	ZMMFNC66A49H703C	12/12/2008

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

e n. 74 (settantaquattro) rapporti di Collaborazione Coordinata e Continuativa:

CO.CO.CO SEDE NAPOLI				
COGNOME/NOME		MATRICOLA	CODICE FISCALE	DATA ASSUNZIONE
ACAMPORA GIOVANNI		000232	CMPGNN74T28F839H	12/11/2009
AMMATURO GIOVANNA		000202	MMTGNN79S68H703V	10/01/2009
AMBRETTI ANTINEA		000217	MBRNTN82C71F839S	23/10/2009
ANNARUMMA MARIA		000000	NNRMRA71C43F912X	23/10/2007
BACARELLA MARIANGELA		000203	BCRMNG86T611438C	10/01/2009
BASILE ALDO		000247	BSL LDA44B27B115J	12/11/2009
BOTTINO ALBERTO		000269	BTTLRT43D19F839E	02/01/2010
BUCCARELLI CRISTIANA MARIA	LE	000204	BCCCST73T64L781V	10/01/2009
CALIENDO GIUDITTA		000246	CLNGTT75T70F839L	12/11/2009
CAPUANO DARIO		000270	CPNDRA82L20F839X	02/08/2010
CIFALDI GIANMARCO		000231	CFLGMR64C27A345S	12/11/2009
CIOFFI MARIA		000205	CFFMRA76H59D755R	10/01/2009
COPPOLA PASQUALE		000206	CPPPQL79C23F839N	10/01/2009
CORONA FELICE		000207	CRNFLC59B26F839K	10/01/2009
CORONA FELICE		000245	CRNFLC59B26F839K	12/11/2009
COTINI RENATO		000271	CTNRNT80E18F839O	02/08/2010
CUCCURULLO FABIO		000223	CCCFA89P08F839L	11/02/2009
D'AURIA MATTHEW		000230	DRAMTH77D20H703T	12/11/2009
DE PIETRO ORLANDO		000244	DPTRND56M25D086Z	12/11/2009
DESIDERIO VIGORITO MICAELA		000208	DSDMCL76L65H703H	10/01/2009
DI IESU MICHELE		000200	DSIMHL70S13F912X	10/01/2009
DI TRAPANI GIOVANNI		000248	DTRGNN72R10F839U	12/11/2009
DI TRAPANI PIERLUIGI		000218	DTRPLG81C24F839N	29/10/2009
ESPOSITO ANTONELLA		000209	SPSNL81A55F839O	10/01/2009
ESPOSITO GIOVANNI		000227	SPSGNN89E03F839O	19/11/2009
FARNETANO PAOLO		000224	FRNPLA74A30A717A	11/04/2009
FERRAIOLO ANNAMARIA		000229	FRRNMR78H571438H	24/11/2009
FRAGNITO MARIO		000243	FRGMRA56B08A509H	12/11/2009
FRATTINI ROBERTO		000219	FRTRRT76R12F839R	29/10/2009
GAGLIONE FILOMENA		000210	GGLFMN82L50B963X	10/01/2009
GALLIANI LUCIANO		000242	GLLLCN43T13D548C	12/11/2009
GESUMMARIA MANRICO		000241	GSMMRC69A09H703U	12/11/2009
GIELLA DOMENICO		000239	GLLDNC51S07H703Z	12/11/2009
GUIDA GIANLUCA		000240	GDUGLC67E12D086G	12/11/2009
IADICICCO ELISABETTA		000211	DCCLBT81T60B963Q	10/01/2009
IANNACCONE SIMONA		000238	NNCSMN78A68A509Q	12/11/2009
IERVOLINO DANILIO		000259	RVL DNL78D02F839W	01/01/2010
IMPARATO ANNAMARIA		000237	MPRNMNR55T45F839E	12/11/2009
IODICE CLAUDIA		000249	DCICLD73T44F839C	12/11/2009
LAUDATI ANNA		000228	LDTNNA73B65H703U	24/11/2009
MAGRI CARLO		000225	MGRCL79B13F839F	11/04/2009

(segue)

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

CO.CO.CO SEDE NAPOLI			
COGNOME/NOME	MATRICOLA	CODICE FISCALE	DATA ASSUNZIONE
MAISTO VINCENZO	000258	MSTVCN85H22H703M	12/11/2009
MARZANO ANTONIO	000262	MRZNTN64H21H703L	19/01/2010
MINELLI MAURO	000256	MNLMRA57H04E506D	12/11/2009
MIRANDA AMALIA	000266	MRNMLA70M68I377O	26/01/2010
MOLINO ADRIANA	000212	MLNDRN75R71A091Q	10/01/2009
MONACO DAVIDE	000226	MNCDVD80C01H703D	11/05/2009
MONTERA LUDOVICO	000250	MNTLVC83L18H703P	12/11/2009
MUSIO IVANA	000260	MSUVNI76H50H703W	19/01/2010
NATALE MARIA	000251	NTLMRA79L59B963Y	12/11/2009
PALLOTTA ERNESTO	000263	PLLRST61D26G273B	19/01/2010
PANZARIELLO ALESSANDRO	000215	PNZLSN75D07H703W	10/01/2009
PAPARELLA NICOLA	000235	PPRNCL40T221158N	12/11/2009
PIERRO ANNA	000274	PRRNA81A47H703E	19/02/2010
PISCOPO CARMINE	000234	PSCCMN35R10H006A	12/11/2009
PISANI CARMELA	000216	PSNCML79D66F912C	10/01/2009
PIU CARMELO	000236	PIUCML42B07A321R	12/11/2009
RUGGIERO DOMENICO GIOVANNI	000252	RGGDNC69A11F839Y	12/11/2009
SABBATO GIOVANNI	000261	SBBGNN66P26H703U	19/01/2010
SANSEVERINO CONCETTA	000222	SNSCCT80P52F839N	29/10/2009
SANTAGATA DE CASTRO RENATO	000254	SNTRNT72R01F839O	12/11/2009
SCARSI GIOVANNA	000272	SCRGNN38S66H703K	18/02/2010
SCHIANO ANNA MARIA	000264	SCHNMR49L67F839Q	19/01/2010
SCOGNAMIGLIO VALENTINA	000267	SCGVNT80B50F839G	26/01/2010
SIANO CATERINA	000268	SNICRN78E45H703T	26/01/2010
SICA ANNAFLORA	000255	SCINFL77D70H703K	12/11/2009
SPEZIGA GIUSEPPINA	000201	SPZGPP84S49H703J	10/01/2009
STIGLIANO UGO	000220	STGGUO81C30F839D	29/10/2009
TRANFAGLIA CARMELINA	000213	TRNCML72T55A509L	10/01/2009
TRAETTA DE BURY GABRIELLA	000224	TRTGRL73M58F839Y	11/02/2009
VALENTINO CATERINA	000265	VLNCRN52P63E932Y	19/01/2010
VENTRE ELVIRA	000233	VNTLVR61P49F839L	12/11/2009
VIOLA ANGELICA	000214	VLINLC70T57F839E	10/01/2009
VITALE ANTONIO	000273	VTLNTN36A14H703Y	18/02/2010
CO.CO.CO SEDE MERCATO SAN SEVERINO (SA)			
COGNOME/NOME	MATRICOLA	CODICE FISCALE	DATA ASSUNZIONE
IANNACCONE ANDREA	000257	NNCNDR81D30A509K	12/11/2009

I dati relativi a tali soggetti sono oggetto di Trattamento da parte dell'Ateneo direttamente o per mezzo di consulente del lavoro:

Studio Professionale Dottor Biagio Napolitano
Via Capua, 52 – 80127 CAMPOSANO (NA)

il quale detiene seppur temporaneamente documentazione e dati del cui trattamento è Titolare l'Ateneo.

A tale soggetto è stata richiesta ed è stata resa apposita dichiarazione scritta in cui viene certificata la conformità del loro sistema informativo e della propria struttura alle previsioni della normativa sulla privacy. Tale dichiarazione è conservata agli atti dell'Ateneo.

(continua)

Tipo di Attività Svolta: Elaborazione Buste Paga

Soggetti Interessati: Lavoratori dipendenti / Familiari dei dipendenti

Tipologia dei Dati Trattati:

DP – Nominativi ed anagrafiche

DS – Documenti atti a rilevare lo stato di salute di tali soggetti

Note: Solo i Dati necessari alla elaborazione delle buste paga vengono mensilmente trasmessi al Consulente del Lavoro per l'elaborazione delle Buste Paga

Luogo fisico di Conservazione: Archivi Fisici

Trasmissione ad altri soggetti: SI – TEMPORANEA

Per l'espletamento delle attività di trattamento dei dati amministrativi relativi ai Clienti/Studenti l'Ateneo utilizza una piattaforma gestionale interna il cui utilizzo comporta il trattamento dei loro dati personali, dal momento che è in grado di elaborare i dati degli studenti ed elaborare report statistici.

La piattaforma studenti funziona tramite web. La trasmissione dei dati relativa alla piattaforma in uso avviene in modo criptato.

attraverso il software è implementato un sistema di **CRM (Customer Relationship Management)** volto a gestire i rapporti con gli studenti a partire dal loro primo contatto con l'Università e fino alla fine della loro carriera, al fine di monitorare e migliorare la loro soddisfazione. Ciò comporta la possibilità che parte dei dati degli studenti sia gestita per finalità di natura statistica, per l'esecuzione di ricerche di mercato, per la definizione e correzione delle iniziative strategiche ed informative, per l'invio di materiale pubblicitario o per il compimento di attività di comunicazione commerciale.

Nelle informative al trattamento dei Dati Personali consegnate agli Studenti nella fase di iscrizione, tale evenienza è chiaramente esplicitata.

Il software **ARXivar** è un sistema per la gestione documentale che consente di archiviare, organizzare e gestire qualunque tipo di informazione sotto forma, nel caso di specie, di documenti word, excel, mail, fax, pdf. Nello specifico, trattasi di un Database cui vengono archiviati direttamente files nativi o derivanti da scansioni eseguite all'interno della struttura.

Per maggiori informazioni in merito al software su descritto si rinvia al sito Internet:

www.abletech.it

(continua)

Per la gestione della didattica e per il monitoraggio del percorso formativo degli studenti viene utilizzato un software sviluppato internamente presso la Unità locale di Salerno: la Piattaforma di erogazione dei corsi a distanza **PegasOnline**.

L'utilizzo del software comporta il trattamento dei loro dati personali.

I server sono amministrati remotamente dalla sede in via S.Vincenzo – Lotto 12 - Mercato S. Severino (Salerno), mediante client OpenSSH, con connessioni cifrate su protocollo DSA a doppia chiave asimmetrica (private key and public key).

Caratteristiche hardware dei server (IBM x-series x336) sono le seguenti:

- Processore (CPU): Xeon
- Frequenza clock processore: 3050MHz
- Front side bus: 833MHz
- Produttore del processore: Intel
- Cache L2 std: 1024 KB
- Memoria(RAM) std/max: 512MB/4096MB
- Velocità RAM: 833MHz
- Tipo RAM: DDR2 ECC SDRAM
- Numeri di dischi fissi installati: 2
- Controller disco fisso: SCSI ServeRaid 6i+ Ultra320
- Tipo disco fisso: SCSI Ultra320
- Hard Disk: HD 2x146.8 GByte (SCSI RAID 1 Ultra320)
- Memoria: 2048 MBytes DDR2 ECC

Tutti i server sono equipaggiati con

- sistema operativo Debian Linux 3.1 stable
- firewall Iptables v1.2.11 stable
- antivirus ClamAV v0.90 stable

I server, laddove previsto, interagiscono tra loro mediante interfacce di rete dedicate (isolate dalla rete esterna) su un canale cifrato basato su protocollo SSL (Secure Socket Layer).

Tutti i dati residenti sugli application server, oltre ad essere preservati in raid 1 (mirroring) su ciascuna macchina, vengono duplicati, mediante task di backup incrementali giornalieri su un Server Dedicato.

L'accesso in piattaforma avviene tramite autenticazione con credenziali (username e password) conservate in un RDBM MySQL in forma crittografata a 256 bit con algoritmo non reversibile (SHA-256).

La generazione delle password avviene in maniera automatica, durante la registrazione degli utenti in piattaforma, mediante algoritmo proprietario.

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

Regola 19.2

Competenze

I Signori sotto elencati, dipendenti o collaboratori interni o esterni dell'Ateneo, sono stati nominati **INCARICATI DEL TRATTAMENTO**

In questo ruolo e nei limiti delle mansioni a loro affidate, essi potranno eseguire le operazioni di trattamento riguardanti le sopradette banche dati, attenendosi alle istruzioni impartite dal titolare del trattamento.

N.	Cognome e Nome	Codice Fiscale	Tipologia Dati	Postazione	Accesso ad Internet	Accesso a Server	Sede di lavoro
1	Giuseppe Mauro	MRAGPP73P29G964S	DP – DS	A	SI	SI	Napoli
2	Livigni Loredana	LVGLDN78B43C495K	DP	B	SI	NO	Napoli
3	De Gaetano Patrizio	DGTPRZ65A15G902M	DP	C	SI	NO (EVENTUALE)	Napoli
4	Palmiero Mario	PLMMRA76D02F839F	DP	D	SI	NO	Napoli
5	Bossa Azzurra	BSSZRR86E67F839D	DP	E	NO	SI	Napoli
6	Sanseverino Concetta	SNSCCT80P52F839N	DP	F	NO	NO	Napoli
7	Donati Maria	DNTMRA73D65F839S	DP	G	SI	NO	Napoli
8	Traetta Gabriella	TRTGRL73M58F839Y	DP	H	SI	NO	Napoli
9	Cuccurullo Fabio	CCCFBA89P08F839L	DP	I	SI	NO	Napoli
10	Cassiani Luna	CSSLNU72B41F839B	DP	L	SI	NO	Napoli
11	Civitillo Daniela	CVTDNL80P49F839N	DP	L	SI	NO	Napoli
12	Di Trapani Pierluigi	DTRPLG81C24F839N	DP	G	SI	NO	Napoli
13	Salzillo Salvatore	SLZSVT80R23B963I	DP - DS	A1	SI	SI	Salerno
14	Falco Filomena	FLCFMN77H45F912Y	DP – DS	B1	SI	SI	Salerno
11	Iannaccone Andrea	NNCNDR81D30A509K	DP	C1	SI	NO	Salerno
12	Matarazzo Modestino	MTRMST83M28A509B	DP	D1	SI	NO	Salerno

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

(continua)

N°	Incaricato al Trattamento		Sede lavoro
13	SANSONE	ANTONIETTA	NAPOLI
14	COLATO	DALILA	NAPOLI
15	DE GAETANO	PATRIZIO	NAPOLI
16	DONATI	MARIA	NAPOLI
17	GARBERINI	DONATA	NAPOLI
18	MUROLO	MASSIMILIANO	NAPOLI
19	VIRZI	GRAZIELLA	NAPOLI
20	BUONOMO	CARMELA	NAPOLI
21	DE SIMONE	GIUSEPPE	SALERNO
22	MARTINIELLO	LUCIA	SALERNO
23	ANNARUMMA	CARMELA	SALERNO
24	MOLINO	ADRIANA	SALERNO
25	VIVONA	ANGELINA	SALERNO
26	CIOFFI	MARIA	SALERNO
27	TEDESCO	INES	SALERNO
28	FEOLA ELVIA	ILARIA	SALERNO
29	SORRENTINO	CLORINDA	SALERNO

N.	Cognome e Nome	Codice Fiscale	Tipologia Dati	Postazione	Accesso ad Internet	Accesso a Server	Sede di lavoro
31	Iervolino Danilo	RVLDNL78D02F839W	DP	H	SI	NO	Napoli
32	Patriota Elio	PRTLEI62M02F839U	DP	I	SI	NO	Napoli
33	Pecorella Gian Giuseppe	PCRGGS60H30H501E	DP - DS	L	NO	SI	Napoli
			DP	LL	SI	NO	

In particolare per i Collaboratori **Pecorella Gian Giuseppe**, **Patriota Elio** e **Iervolino Danilo** si segnala che essi non hanno limiti di alcun tipo né software né hardware, dato il ruolo che rivestono nell'ambito dell'Organizzazione e sempre nei limiti del raggiungimento dei fini sociali.

Tuttavia, per esigenze di sicurezza, lavorano su postazioni Stand – alone e quindi non connesse al Server.

L' Università telematica Pegaso, attualmente, utilizza un totale di 10 sistemi informativi.

Il trattamento di tutti i Dati di cui alla Regola 19.1, effettuato all'interno dell'Ateneo, avviene mediante la seguente strumentazione.

Le attività dell'Ateneo sono organizzate nei locali indicati nella planimetria allegata mentre i software, rilevanti ai fini del trattamento di dati, utilizzati da ciascun PC sono di seguito descritti:

Unità Locale: Napoli - Ufficio: Presidenza – Utente: Danilo Iervolino

PC

Componente	Specifica Tecnica
Processore:	PIV 3 hz
Ram:	1MB
Hard Disk:	203 Ghz

Connessioni disponibili:

Tipo	Motivazione
Internet	Si – Giustifica successivamente il traffico effettuato
Telefonate s/abbreviate:	Per elevato traffico (giustifica successivamente le telefonate effettuate)

Software Installati:

Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office 2003	Stesura documenti
Adobe Reader	Lettura documenti
Skype	Relazioni esterne
AlZip	Decompressione files

Unità Locale: Napoli - Ufficio: Amministrazione – Utente: Gian Giuseppe Pecorella

PC

Componente	Specifica Tecnica
Processore:	T2399 1,66 Ghz
Ram:	540 MB
Hard Disk:	60 GB

Connessioni disponibili:

Tipo	Motivazione
Internet	Visualizzazione siti relativi a regolamenti aziendali – Giustifica successivamente il traffico effettuato
Telefonate s/abbreviate:	Per elevato traffico (giustifica successivamente le telefonate effettuate)

Software Installati:

Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office 2003	Stesura Documenti
Arxivar	Gestione Pratiche

Ps. L'utente usufruisce di un collegamento esterno alla rete aziendale, tramite postazione dedicata, per attività amministrative.

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

Unità Locale: Napoli - Ufficio: Ced – Utente: Giuseppe Mauro

PC

Componente	Specifica Tecnica
Processore:	PIV 3,2 Mhz
Ram:	1MB
Hard Disk:	203 Ghz

Connessioni disponibili:

Tipo	Motivazione
Internet	Si – Amministratore di Sistema
Telefonate s/abbreviate:	Per elevato traffico (giustifica successivamente le telefonate effettuate)

Software Installati:

Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office 2003	Stesura documenti
Skype	Relazioni esterne
AIZip	Decompressione files
Alleycode	Stesura pagine Web
Nero 7	Masterizzazione
Filezilla	FTP
Power DVD	Visualizzazione File Multimediali
OpeOffice	Stesura documenti
Adobe Full	Stesura documenti PDF
Arxivar	Software gestione pratiche

Unità Locale: Napoli - Ufficio: ECP

PC

Componente	Specifica Tecnica
Processore:	P4 2.66 GHZ
Ram:	224 MB
Hard Disk:	38,2 GB

Connessioni disponibili:

Tipo	Motivazione
Internet:	X Controllo Manifestazioni ECP – Giustifica successivamente il traffico effettuato
Telefonate s/abbreviate:	Per elevato traffico (giustifica successivamente le telefonate effettuate)

Software Installati:

Nome	Motivazione
Windows XP SP2	Sistema Operativo
Adobe Flash Player Active X	Per Visualizzazione animazioni siti
Adobe Reader 7.0	Per visualizzazione documenti pdf
Adobe Shockwave Player	Per Visualizzazione animazioni siti
Google Hearth	Orientamento Stradale
Open Office	Stesura Documenti

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

Unità Locale: Napoli - Ufficio: ECP – Utente: Mario Palmiero	
PC	
Componente	Specifica Tecnica
Processore:	P4 3 GHZ
Ram:	1 GB
Hard Disk:	189 GB
Connessioni disponibili:	
Tipo	Motivazione
Internet:	X Controllo Manifestazioni ECP– Giustifica successivamente il traffico effettuato
Telefonate s/abbreviate:	Per elevato traffico (giustifica successivamente le telefonate effettuate)
Software Installati:	
Nome	Motivazione
Windows XP SP2	Sistema Operativo
Adobe F. Player Active X	Per Visualizzazione animazioni siti
Adobe Reader 7.0	Per visualizzazione documenti pdf
ALLZip	Per decompressione files
Adobe Shockwave Player	Per Visualizzazione animazioni siti
Google Hearth	Orientamento Stradale
Office 2003	Stesura Documenti
VideoLan	Visualizzare video da dvd ecp
Postit reminder	Ricorda appuntamenti
Open Office	Stesura Documenti
Unità Locale: Napoli - Ufficio: Commerciale – Utente: Loredana Livigni	
PC	
Componente	Specifica Tecnica
Processore:	P4 3 GHZ
Ram:	1 GB
Hard Disk:	189 GB
Connessioni disponibili:	
Tipo	Motivazione
Internet:	X Controllo Manifestazioni legate ad attività Commerciali – Giustifica successivamente il traffico effettuato
Telefonate s/abbreviate:	Per elevato traffico (giustificano successivamente le telefonate effettuate)
Software Installati:	
Nome	Motivazione
Windows XP SP2	Sistema Operativo
Adobe Flash Player Active X	Per Visualizzazione animazioni siti
Open Office	Stesura Documenti
Unità Locale: Napoli - Ufficio: Call Center/Segreteria – Utente: Azzurra Bossa	
PC	
Componente	Specifica Tecnica
Processore:	P4 3 GHZ
Ram:	1 GB
Hard Disk:	189 GB
Connessioni disponibili:	
Tipo	Motivazione
Telefonate c/abbreviate:	Non ha contatti esterni
Connessione ad Internet	NO
Software Installati:	
Nome	Motivazione
Windows XP SP2	Sistema Operativo
Arxivar	Software avanzamento Pratiche
Open Office	Stesura Documenti

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

Unità Locale: Napoli - Utente: Elio Pariota	
PC	
Componente	Specifica Tecnica
Processore:	PIV 3 hz
Ram:	1MB
Hard Disk:	203 Ghz
Connessioni disponibili:	
Tipo	Motivazione
Internet	Si – Ricerche di Marketing – Giustifica successivamente il traffico effettuato
Telefonate s/abbreviate:	Per elevato traffico (giustifica successivamente le telefonate effettuate)
Software Installati:	
Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office 2003	Stesura documenti
Adobe Reader	Lettura documenti
Skype	Relazioni esterne
AlZip	Decompressione files
Google Hearth	Orientamento Stradale
Unità Locale: Napoli - Ufficio: Commerciale	
PC	
Componente	Specifica Tecnica
Processore:	P4 3 GHZ
Ram:	1 GB
Hard Disk:	196 GB
Connessioni disponibili:	
Tipo	Motivazione
Internet	X Controllo Manifestazioni legate ad attività Commerciali – Giustifica successivamente il traffico effettuato
Telefonate s/abbreviate:	Per elevato traffico (giustifica successivamente le telefonate effettuate)
Software Installati:	
Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office 2003	Stesura Documenti
OpenOffice	Stesura Documenti
Post It	Promemoria
Nero	Masterizzazioni
AlZip	Decompressione Files
Video Lan	Visualizzazione files multimediali.
CCleaner	Miglioramento registro di sistema

**Unità Locale: Salerno - Ufficio: Analista programmatore
Utente: Sig. Salvatore Salzillo**

<u>UTENTE</u>	<u>HARDWARE</u>	<u>SOFTWARE</u>
Salvatore Salzillo	<ul style="list-style-type: none"> ● Intel® Core™ 2 Duo E6700 ● DDR2 2Gb ECC registred ● 128MB nVidia Quadro FX540 Graphics Card ● 250GB SATA First Hard Drive ● 250GB SATA Second Hard Drive ● DVD+/-RW Drive ● DVD Drive ● Floppy Disk ● 3.5in 1.44MB Floppy Drive ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità <p align="center"><u>CONNESSIONI DISPONIBILI</u></p> INTERNET: SI TELEFONATE: SI	<ul style="list-style-type: none"> ● Gentoo Linux 2006.1 ● Iptables Firewall

Unità Locale: Salerno - Ufficio: Archivist
Utente:

<u>UTENTE</u>	<u>HARDWARE</u>	<u>SOFTWARE</u>
	<ul style="list-style-type: none"> ● CPU Intel® P4 3200 ● RAM1 DDR2 PC533 1Gb ● RAM2 DDR2 PC533 1Gb ● Masterizzatore DVD ● Lettore DVD ● Floppy Disk ● Sheda video Nvidia GeForce 6600V+ ● HD 200Gb SATA Maxtor ● Case Enermax 350W ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità <p align="center"><u>CONNESSIONI DISPONIBILI</u></p> INTERNET: SI TELEFONATE: SI	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Pinnacle studio 10 ● Adobe Premiere ● Microsoft Office 2007 ● Ahead Nero 7 ● Macromedia Studio 8

Sede Legale: Napoli

Ufficio: Amministrazione – Utente: Gian Giuseppe Pecorella

PC

Componente	Specifica Tecnica
Processore:	T2399 1,66 Ghz
Ram:	540 MB
Hard Disk:	60 GB

Connessioni disponibili:

Tipo	Motivazione
Internet	Visualizzazione siti relativi a regolamenti aziendali – Giustifica successivamente il traffico effettuato
Telefonate s/abbreviate:	Per elevato traffico (giustifica successivamente le telefonate effettuate)

Software Installati:

Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office 2003	Stesura Documenti
Arxivar	Gestione Pratiche

Ps. L'utente usufruisce di un collegamento esterno alla rete aziendale, tramite postazione dedicata, per attività amministrative.

Ufficio: Segreteria – Utente: Antonietta Sansone

PC

Componente	Specifica Tecnica
Processore:	PIV 1.85 Ghz
Ram:	224 MB
Hard Disk:	40 GB

Connessioni disponibili:

Tipo	Motivazione
Internet	SI, limitatamente al Sito Istituzionale www.unipegaso.it
Telefonate s/abbreviate:	NO – Non ha contatti esterni

Software Installati:

Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office XP	Stesura documenti
Adobe Reader	Lettura documenti

Ufficio: Segreteria – Utente: Fabio Cuccurullo

PC

Componente	Specifica Tecnica
Processore:	PIV 1.85 Ghz
Ram:	224 MB
Hard Disk:	40 GB

Connessioni disponibili:

Tipo	Motivazione
Internet	SI, limitatamente al Sito Istituzionale www.unipegaso.it
Telefonate s/abbreviate:	NO – Non ha contatti esterni

Software Installati:

Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office XP	Stesura documenti
Adobe Reader	Lettura documenti

Ufficio: Segreteria – Utente: Colato Dalila – Virzì Gabriella	
PC	
Compenente	Specifica Tecnica
Processore:	PIV 1.85 Ghz
Ram:	224 MB
Hard Disk:	40 GB
Connessioni disponibili:	
Tipo	Motivazione
Internet	SI, limitatamente al Sito Istituzionale www.unipegaso.it
Telefonate s/abbreviate:	NO – Non ha contatti esterni
Software Installati:	
Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office XP	Stesura documenti
Adobe Reader	Lettura documenti
Ufficio Amministrativo: Buonomo Carmela – Garberini Donata – De Gaetano Patrizio – Donati Maria	
PC	
Compenente	Specifica Tecnica
Processore:	PIV 1.85 Ghz
Ram:	224 MB
Hard Disk:	40 GB
Connessioni disponibili:	
Tipo	Motivazione
Internet	SI, limitatamente al Sito Istituzionale www.unipegaso.it
Telefonate s/abbreviate:	NO – Non ha contatti esterni
Software Installati:	
Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office XP	Stesura documenti
Adobe Reader	Lettura documenti
Ufficio ECP: Murolo Massimiliano	
PC	
Compenente	Specifica Tecnica
Processore:	PIV 1.85 Ghz
Ram:	224 MB
Hard Disk:	40 GB
Connessioni disponibili:	
Tipo	Motivazione
Internet	SI, limitatamente al Sito Istituzionale www.unipegaso.it
Telefonate s/abbreviate:	NO – Non ha contatti esterni
Software Installati:	
Nome	Motivazione
Windows XP SP2	Sistema Operativo
Office XP	Stesura documenti
Adobe Reader	Lettura documenti

<u>Unità locale di Mercato San Severino (SA)</u>		
	Caratteristiche Hardware	Caratteristiche Software
Lucia Martiniello	<ul style="list-style-type: none"> ● CPU Intel® P4 3200 ● RAM1 DDR2 PC533 1Gb ● RAM2 DDR2 PC533 1Gb ● Masterizzatore DVD ● Lettore DVD ● Floppy Disk ● Scheda video Nvidia GeForce 6600V+ ● HD 200Gb SATA Maxtor ● Case Enermax 350W ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità 	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Microsoft Office 2007 ● Ahead Nero 7 ● AVG Internet Security (Antivirus + AntiSpyware + AntiSpam + Firewall)
Maria Annarumma	<ul style="list-style-type: none"> ● CPU Intel® P4 3200 ● RAM1 DDR2 PC533 1Gb ● RAM2 DDR2 PC533 1Gb ● Masterizzatore DVD ● Lettore DVD ● Floppy Disk ● Scheda video Nvidia GeForce 6600V+ ● HD 200Gb SATA Maxtor ● Case Enermax 350W ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità 	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Microsoft Office 2007 ● Ahead Nero 7 ● AVG Internet Security (Antivirus + AntiSpyware + AntiSpam + Firewall)
Giuseppe De Simone	<ul style="list-style-type: none"> ● Intel® Core™ 2 Duo E6700 ● DDR2 2Gb ECC registred ● Ati V3300 FireGL 128Mb ● 250GB SATA First Hard Drive ● 250GB SATA Second Hard Drive ● DVD+/-RW Drive ● Floppy Disk ● 3.5in 1.44MB Floppy Drive ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità 	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Microsoft Office 2007 ● Macromedia Studio 8 ● Ahead Nero 7 ● Pinnacle Studio 10 ● Camtasia ● Adobe Elements ● Macromedia Director ● AVG Internet Security (Antivirus + AntiSpyware + AntiSpam + Firewall)
Angela Vivona	<ul style="list-style-type: none"> ● CPU Intel® P4 3200 ● RAM1 DDR2 PC533 1Gb ● RAM2 DDR2 PC533 1Gb ● Masterizzatore DVD ● Lettore DVD ● Floppy Disk ● Scheda video Nvidia GeForce 6600V+ ● HD 200Gb SATA Maxtor ● Case Enermax 350W ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità 	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Microsoft Office 2007 ● Macromedia Studio 8 ● Ahead Nero 7 ● AVG Internet Security (Antivirus + AntiSpyware + AntiSpam + Firewall)
Elvia Feola	<ul style="list-style-type: none"> ● CPU Intel® P4 3200 ● RAM1 DDR2 PC533 1Gb ● RAM2 DDR2 PC533 1Gb ● Masterizzatore DVD ● Lettore DVD ● Floppy Disk ● Scheda video Nvidia GeForce 6600V+ ● HD 200Gb SATA Maxtor ● Case Enermax 350W ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità 	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Microsoft Office 2007 ● Macromedia Studio 8 ● Ahead Nero 7 ● AVG Internet Security (Antivirus + AntiSpyware + AntiSpam + Firewall)

Unità locale di Mercato San Severino (SA) (segue)

	Caratteristiche Hardware	Caratteristiche Software
Maria Cioffi	<ul style="list-style-type: none"> ● CPU Intel® P4 3200 ● RAM1 DDR2 PC533 1Gb ● RAM2 DDR2 PC533 1Gb ● Masterizzatore DVD ● Lettore DVD ● Floppy Disk ● Scheda video Nvidia GeForce 6600V+ ● HD 200Gb SATA Maxtor ● Case Enermax 350W ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità 	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Microsoft Office 2007 ● Macromedia Studio 8 ● Ahead Nero 7 ● AVG Internet Security (Antivirus + AntiSpyware + AntiSpam + Firewall)
Clorinda Sorrentino	<ul style="list-style-type: none"> ● CPU Intel® P4 3200 ● RAM1 DDR2 PC533 1Gb ● RAM2 DDR2 PC533 1Gb ● Masterizzatore DVD ● Lettore DVD ● Floppy Disk ● Scheda video Nvidia GeForce 6600V+ ● HD 200Gb SATA Maxtor ● Case Enermax 350W ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità 	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Microsoft Office 2007 ● Macromedia Studio 8 ● Ahead Nero 7 ● AVG Internet Security (Antivirus + AntiSpyware + AntiSpam + Firewall)
Adriana Molino	<ul style="list-style-type: none"> ● CPU Intel® P4 3200 ● RAM1 DDR2 PC533 1Gb ● RAM2 DDR2 PC533 1Gb ● Masterizzatore DVD ● Lettore DVD ● Floppy Disk ● Scheda video Nvidia GeForce 6600V+ ● HD 200Gb SATA Maxtor ● Case Enermax 350W ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità 	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Microsoft Office 2007 ● Macromedia Studio 8 ● Ahead Nero 7 ● AVG Internet Security (Antivirus + AntiSpyware + AntiSpam + Firewall)
Ines Tedesco	<ul style="list-style-type: none"> ● CPU Intel® P4 3200 ● RAM1 DDR2 PC533 1Gb ● RAM2 DDR2 PC533 1Gb ● Masterizzatore DVD ● Lettore DVD ● Floppy Disk ● Scheda video Nvidia GeForce 6600V+ ● HD 200Gb SATA Maxtor ● Case Enermax 350W ● Monitor Samsung SM9013V TFT 19" ● UPS Gruppo di Continuità 	<ul style="list-style-type: none"> ● Microsoft Windows Xp Professional ● Microsoft Office 2007 ● Macromedia Studio 8 ● Adobe Photoshop css 2 ● Ahead Nero 7 ● Adobe Illustrator ● AVG Internet Security (Antivirus + AntiSpyware + AntiSpam + Firewall)

Regola 19.3

Analisi Rischi

Regola 19.4.1

Misure

di Sicurezza

adottate

Analisi dei Rischi

Ad un livello generale sono state individuate le seguenti principali minacce alla sicurezza dei dati gestiti dall'Ateneo suddivise in tre macrocategorie:

Calamità naturali	Minacce intenzionali	Minacce involontarie
Terremoto Incendio Fulmine	Accessi non autorizzati Virus informatici Furto di dati e di attrezzature hardware	Black out elettrico Malfunzionamenti nel software Malfunzionamenti hardware Errori umani nell'utilizzo del sistema informatico dell'Ateneo

In riferimento alla sicurezza dei dati personali gestiti l'Ateneo si pone i seguenti obiettivi:

Obiettivo:	Cosa significa:
<u>riservatezza</u>	I dati devono essere accessibili solo alle persone autorizzate
<u>integrità</u>	I dati devono essere protetti da modificazioni e danneggiamenti
<u>disponibilità</u>	I dati devono essere accessibili alle persone autorizzate

Attraverso l'implementazione di una serie di misure di sicurezza, espone in dettaglio nei successivi paragrafi, si vuole ridurre le vulnerabilità del sistema informativo dell'Ateneo, raggiungendo un livello di rischio valutato accettabile.

In sintesi:

Tutelare l'obiettivo:	significa:
<u>riservatezza</u>	Ridurre il rischio che persone non autorizzate possano accedere alle informazioni
<u>Integrità</u>	Ridurre il rischio che le informazioni siano non volutamente modificate o cancellate
<u>disponibilità</u>	Ridurre il rischio di non poter accedere anche se autorizzati alle informazioni

Rischio: sottrazione di Credenziali di Autenticazione

Impatto sulla Sicurezza: Possibilità che Utenti Trattano Dati per cui non abbiano Autorizzazione

Gravità: Media

Misure di Sicurezza Adottate: Utilizzo di Sistemi di crittografia per la registrazione delle credenziali di autenticazione

Rischio: Errore Materiale

Impatto sulla Sicurezza: Perdita dei Dati

Gravità: Bassa

Misure di Sicurezza Adottate: Adozione di metodiche e procedure lavorative adeguate. Formazione del personale. Procedure di backup periodiche

Rischio: Azione di Virus Informatici o di programmi suscettibili di recare danno. Spamming od altre tecniche di sabotaggio Informatico

Impatto sulla Sicurezza: Perdita dei Dati o Danneggiamento e sottrazione degli stessi

Gravità: Medio-bassa

Misure di Sicurezza Adottate: Adozione di software Antivirus e Firewall e di software AntiSpam ed AntiSpyware e costante aggiornamento dello stesso.

Analisi dei Rischi

(continua)

Rischio: Malfunzionamento, indisponibilità e degrado degli strumenti
Impatto sulla Sicurezza: Inadeguatezza degli strumenti utilizzati per la protezione in funzione del processo tecnologico

Gravità: Bassa

Misure di Sicurezza Adottate: Costante aggiornamento dei software utilizzati per la gestione dei dati. Costante adeguamento della strumentazione obsoleta

Rischio: accessi esterni telematici non autorizzati

Impatto sulla Sicurezza: in presenza di connessione Internet il rischio è la sottrazione di dati sensibili

Gravità: Bassa

Misure di Sicurezza Adottate: Dotazione di Linea ADSL, Adozione di un sistema Firewall, Aggiornamento del sistema operativo, controllo dell'amministratore di sistema.

Rischio: accessi non autorizzati ad Aree e Zone dell'Ateneo ad accesso ristretto

Impatto sulla Sicurezza: Sottrazione fisica dei dati

Gravità: bassa

Misure di Sicurezza Adottate: Limitazione e controllo degli accessi. Presenza del PC in Stanza operativa. Presenza di Porte per l'accesso alle Aree Operative e Direzionali, documenti cartacei conservati in dei mobili chiusi a chiave.

Rischio: Sottrazione di Strumenti contenenti i Dati

Impatto sulla Sicurezza: Perdita dei Dati

Gravità: Bassa

Misure di Sicurezza Adottate: L'accesso alle Aree Operativa e Direzionale è protetto da porte. Gli accessi sono limitati

Rischio: Eventi distruttivi naturali od artificiali nonchè dolosi accidentali o dovuti ad incuria

Impatto sulla Sicurezza: Perdita dei Dati

Gravità: Bassa

Misure di Sicurezza Adottate: Procedure di backup periodiche

Rischio: Guasto ai sistemi complementari (impianto elettrico ecc ecc)

Impatto sulla Sicurezza: Perdita dei Dati o Danneggiamento

Gravità: Bassa

Misure di Sicurezza Adottate: Gruppo di Continuità. Procedure di Backup periodiche

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

Regola 19.4.2

*Scheda
Descrittiva
delle
Misure di
Sicurezza*

Regola 19.5

*Criteri e
Procedure*

Scheda descrittiva delle Misure di Sicurezza

- L'accesso alle due unità locali è custodito;
- La sedi sono protette da sistema di Allarme;
- Tutti i PC ed i Server sono protetti da Password;
- L'accesso fisico alle stanze contenenti documenti trattanti dati personali è permesso solo ai soggetti Incaricati;
- Gli armadi in cui sono detenuti documenti cartacei inerenti dati personali non sono accessibili a personale non incaricato e la stanza ove sono custoditi è protetta da serrature;
- I documenti cartacei inerenti i dati sensibili dei dipendenti sono conservati temporaneamente presso lo Studio Professionale incaricato.

Gestione strumenti elettronici

Backup dati

Al fine di garantire non solo la integrità, ma anche la pronta disponibilità dei dati, l'Ateneo si è dotato di strumenti e procedure di backup.

È stato scelto un server esterno, collegato in rete, come strumento di backup principale dell'Ateneo. Per ulteriori informazioni è possibile visitare il sito <http://webfarm.aruba.it> per l'unità di Napoli.

Per l'unità di **Mercato San Severino**, come descritto alla pagina 16, la Piattaforma di erogazione dei corsi a distanza PegasOnline è residente su molteplici server indipendenti, tutti locati fisicamente presso il **Datacenter carrier class di Seeweb s.r.l. in Via Caldera, 21 – Milano.**

Si è valutata la modalità di backup e la capacità di memoria del Server esterno più che sufficiente per la mole di dati attualmente gestita dall'Ateneo stesso.

Tutti i dati personali gestiti con strumenti elettronici dall'Ateneo vengono inclusi nella procedura di backup. La frequenza con cui vengono effettuate le copie di sicurezza è settimanale, solitamente il venerdì mattina.

I responsabili del trattamento, sono stati incaricati a gestire le copie di sicurezza e le procedure di backup.

Il tempo massimo per la conservazione delle copie di backup è stato stabilito in 1 mese.

Il tempo necessario per recuperare i dati delle copie di sicurezza, a fronte di una generica emergenza, viene stimato in poche ore dal verificarsi del possibile accadimento negativo, comunque ampiamente sotto il limite dei sette giorni previsti dal punto 23 dell'allegato B del D.Lgs. 196/2003 in ipotesi di trattamento di dati sensibili.

Scheda descrittiva delle Misure di Sicurezza (...)

Antivirus

L'Ateneo si è dotato del software **Bit Defender Antivirus** che è stato installato sulle diverse postazioni Client o Server che accedono ad Internet.

Le caratteristiche principali di **Bit Defender Antivirus** includono:

- **Malware come virus, worms, trojans ed altri.** BitDefender protegge il vostro computer da ogni tipo di minaccia malware (virus, troiani, spyware, rootkit ed altro).
- **Infezioni del computer** BitDefender protegge usando programmi per chat (tipo ICQ, MSN, etc.) e software per scambiare dati (p.e. BitTorrent) **Software di spionaggio e pubblicità indesiderata (SPAM)** BitDefender esegue il monitoraggio di dozzine di potenziali "hotspots" nel vostro sistema dove lo spyware potrebbe agire; inoltre analizza qualsiasi cambiamento avvenuto sia nel sistema che sul software. Le minacce dello spyware sono quindi bloccate in tempo reale. Il modulo è attivo e blocca Trojan o altri codici installati da hackers, nel tentativo di compromettere la vostra privacy inviando informazioni personali, quali numeri di carte di credito per esempio, dal vostro computer ad altri.
- **Virus sconosciuti** BitDefender usa la tecnologia B-HAVE (Behavioural Heuristic Analyser in Virtual Environments) per proteggere da virus nuovi non ancora conosciuti.
- **Pericoli nascosti (rootkits)** I rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e log ed evitare il rilevamento. BitDefender aiuta di rintracciare ed eliminare i rootkit.
- **Attacchi phishing** Phishing è un'attività criminale su Internet che utilizza tecniche sociali d'ingegneria per indurre la gente con l'inganno a fornire informazione personale. I principali obiettivi del phishing sono i clienti dei servizi di pagamento on line, come eBay e PayPal, come anche le banche che offrono servizi on line. Recentemente, anche gli utenti di siti web di reti sociali sono stati presi di mira dal phishing per ottenere dati d'identificazione personale usati poi per il furto d'identità. Per essere protetti dai tentativi antiphishing quando navigate su Internet, mantenere Antiphishing attivo.
- **Update ogni ora** Tutti i giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

L'aggiornamento del prodotto antivirus installato è continuo e fatto automaticamente tramite una funzionalità a disposizione nel prodotto stesso.

L'antivirus in oggetto controlla in automatico ogni file scaricato dalla rete o dalla posta elettronica o letto da supporti esterni quali floppy disk e cd-rom.

Il personale è stato adeguatamente informato sui comportamenti corretti da tenere per evitare di introdurre virus informatici nell'Ateneo professionale come evidenziato nel regolamento allegato.

I responsabili sono stati incaricati di seguire il corretto aggiornamento del software antivirus.

Aggiornamento sistema operativo

I responsabili sono stati incaricati di seguire il corretto e frequente aggiornamento del sistema operativo attraverso funzionalità del sistema operativo stesso e degli eventuali altri software utilizzati correntemente.

Gruppi di continuità

La dotazione hardware comprende Gruppi di continuità per i PC ed i Server utilizzati all'interno dell'Ateneo per prevenire le conseguenze dei blackout elettrici o dei picchi di sovra o sotto tensione elettrica. Il gruppo di continuità in oggetto è in grado di filtrare l'alimentazione elettrica da eventuali impurità.

Firewall e sistemi di anti intrusione

La protezione firewall è garantita dal sistema operativo windows XP.

Gestione supporti rimovibili contenenti dati sensibili

Nel regolamento operativo allegato sono state fornite istruzioni organizzative e tecniche ad hoc per la custodia e l'uso di eventuali supporti rimovibili contenenti dati sensibili (floppy disk, chiavette hard disk, cd riscrivibili, ecc.).

Sistema di identificazione e autenticazione

L'Ateneo ha attivato ed è correntemente funzionante un sistema d'autenticazione per ognuno degli incaricati che trattano dati personali.

È stato attribuito un codice identificativo (**username, user ID**) strettamente personale per l'utilizzazione degli strumenti elettronici (di solito personal computer) del sistema informatico.

I codici identificativi sono frequentemente aggiornati, inserendo quelli dei nuovi incaricati e cancellando quelli degli incaricati non più autorizzati.

Il sistema di autenticazione prevede l'utilizzo di parole chiave (**password**) sia a livello di sistema operativo sia a livello di singola applicazione.

I responsabili sono stati incaricati della gestione delle password nell'Ateneo.

Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso. Si sollecita l'incaricato che riceve una password a modificarla al primo utilizzo.

Ai sensi del D.Lgs. 196/03 viene segnalata ad ogni incaricato la necessità di cambiare la password almeno ogni 6 mesi.

Nell'ipotesi di trattamento di dati sensibili viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 3 mesi.

Scheda descrittiva delle Misure di Sicurezza

Sistema di identificazione e autenticazione

È prevista una scadenza nella validità di ogni password utilizzata.

Sono vietate credenziali di autenticazione (username e password) condivise fra più persone.

Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate. Le credenziali di autenticazione vengono immediatamente revocate in caso di provvedimenti disciplinari o quando si presentano situazioni che possono compromettere la sicurezza.

Sono state consegnate istruzioni scritte agli incaricati in merito alle modalità di gestione e di custodia delle password.

La visualizzazione della password sullo schermo dei personal computer è impedita da tutti i software in uso.

Documento Programmatico sulla Sicurezza (DPS) ANNO 2010

Regola 19.6

Formazione

Business continuity plan e disaster recovery plan

In conseguenza della limitata dimensione e della bassa complessità dell'Ateneo non si valuta necessario procedere all'elaborazione formale di tali documenti.

Si valuta che le misure di sicurezza attualmente implementate e gestite, esplicitate in questo documento, siano sufficienti per poter ripristinare il sistema informativo dell'Ateneo in tempi brevi e a costi contenuti al verificarsi di emergenze o di eventi negativi.

Regola 19.7

Trattamenti

Affidati

All'esterno

Trattamenti di dati personali affidati all'esterno della struttura dell'Ateneo

Alla data di redazione del presente documento, rilevano trattamenti di dati personali e sensibili affidati all'esterno ed in particolare a n. 2 (due) collaboratori esterni.

A tali soggetti, in qualità di Collaboratori esterni è stata richiesta ed è stata resa apposita dichiarazione scritta in cui viene certificata la conformità del loro sistema informativo alle previsioni della normativa sulla privacy. Tale dichiarazione è conservata agli atti dell'Ateneo.

Nell'ipotesi vi fosse necessità di affidare altri trattamenti di dati personali all'esterno, per esempio ad altri colleghi professionisti, va richiesta a tali soggetti una specifica dichiarazione scritta in cui viene certificata la conformità del loro sistema informativo alle previsioni della normativa sulla privacy.

Regola 19.5

Cifatura

Trattamenti senza l'ausilio di strumenti elettronici

Nella sezione "**gestione documenti cartacei**" del Regolamento di utilizzo degli strumenti elettronici allegato al presente documento, sono impartite agli incaricati istruzioni scritte, finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Il responsabile del trattamento è incaricato della gestione delle autorizzazioni nei luoghi contenenti archivi di dati sensibili.

Formazione

L'Ateneo riconosce l'importanza della formazione dei suoi componenti riguardo le tematiche della sicurezza, come elemento significativo di riduzione dei rischi al proprio sistema informativo e s'impegna a promuovere momenti formativi, in particolare al momento dell'ingresso in servizio o al momento di cambiamenti di mansioni di tali soggetti o all'introduzione di nuovi strumenti elettronici che hanno impatto sul trattamento dei dati personali.

Tutti i componenti dell'Ateneo devono comunque partecipare una volta all'anno ad un corso di approfondimento e mantenimento delle conoscenze in materia di sicurezza informatica in aula o in modalità e-learning dalla durata di mezza giornata.

Modalità aggiornamento del documento programmatico per la sicurezza

Il responsabile del trattamento è il soggetto preposto all'aggiornamento e alla custodia del documento programmatico per la sicurezza.

Il documento in oggetto non deve rimanere statico ma deve essere aggiornato ogni volta che vi siano cambiamenti significativi nell'Ateneo impattanti sulle misure minime di sicurezza.

Napoli, 01 marzo 2010