

**Pos. UL**

**Decreto n. 860**

**IL RETTORE**

VISTO il Decreto legislativo 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali", con particolare riferimento agli articoli 18, 20, 21, 22 e 181, comma 1, lett. a);

VISTA la deliberazione n. 13 del 20 dicembre 2005, con la quale il Consiglio di Amministrazione ha approvato il Documento programmatico per la Sicurezza dell'Università degli Studi di Napoli Parthenope;

VISTA la deliberazione n. 14 del 20 dicembre 2005, con la quale il Consiglio di Amministrazione ha approvato lo schema di Regolamento per l'utilizzo delle risorse informatiche e l'accesso alla rete e ai servizi di rete di Ateneo, che costituisce necessario completamento degli adempimenti di cui al citato Dlgs.196/2003, nonché logico svolgimento del predetto Documento programmatico per la Sicurezza dell'Università degli Studi di Napoli Parthenope;

VISTO l'art. 7 dello Statuto

**DECRETA**

ART. 1 E' emanato il Regolamento per l'utilizzo delle risorse informatiche e l'accesso alla rete e ai servizi di rete di Ateneo nel testo allegato al presente decreto del quale costituisce parte integrante.

ART. 2 Il presente Regolamento entra in vigore il quindicesimo giorno successivo alla sua pubblicazione all'albo dell'Ateneo.

Napoli, 29 dicembre 2005

**IL RETTORE**  
(Prof. Gennaro Ferrara)

# **Regolamento per l'utilizzo delle risorse informatiche e l'accesso alla rete ed ai servizi di rete dell'Ateneo**

Approvato dalla Commissione per la Sicurezza Informatica il 19.12.2005

Approvato dal Consiglio di Amministrazione il 20.12.2005

Emanato con Decreto Rettoriale n. 860 del 29.12.2005

## **1.0 Generalità e definizioni**

Il presente Regolamento normalizza la gestione, il funzionamento, l'accesso e l'uso sicuri delle risorse informatiche dell'Università degli Studi di Napoli "Parthenope".

### **1.1 Prefazione**

La necessità di regolamentare l'accesso e l'uso delle risorse informatiche dell'Ateneo deriva da un più generale contesto che, partendo dalle circolari del CNIPA e dalle linee guida emanate dagli organismi internazionali, ha prodotto una serie di leggi e decreti in tema di trasmissione delle informazioni e di sicurezza informatica. La vigente normativa riconosce, infatti, un ruolo centrale e strategico alle nuove tecnologie informatiche nello sviluppo e nel potenziamento dei servizi offerti dall'Amministrazione Pubblica e, nel contempo, sottolinea il problema della gestione dei potenziali fattori di rischio connessi con tali tecnologie: l'affidabilità del mezzo e la disponibilità, integrità e riservatezza delle informazioni, non lasciando alcuna discrezionalità nell'adozione di efficaci misure atte a prevenire o minimizzare i rischi di incidente informatico o di atti di pirateria informatica.

Si è pertanto ritenuto necessario normalizzare l'accesso alle risorse informatiche non solo per il loro ruolo strategico e la crescente importanza delle tecnologie informatiche, ma anche per la modifica del codice penale che ha introdotto i crimini informatici, la recente normativa antiterrorismo che sottolinea l'importanza della tracciabilità delle trasmissioni, ed il grave danno di immagine per l'Ateneo nel caso di incidente informatico. La qualità dei servizi offerti, infatti, non può prescindere dalla sicurezza della rete e comportamenti non armonizzati costituiscono quantomeno una fonte di rischio per il normale svolgimento dell'attività istituzionali, con eventuali conseguenze di tipo civile e penale, anche solo nel caso si rilevi un reato omissivo (art. 40 c.p.).

L'implementazione di misure di sicurezza, infine, non va considerata come un aggravio della normale attività lavorativa, ma come uno strumento per migliorare la qualità complessiva dei servizi offerti dall'Università, e la sicurezza della rete e dei servizi di rete di Ateneo deve basarsi su principi di elevata disponibilità ed efficienza, in un contesto di armonizzazione degli stessi e di compatibilità con le normative vigenti e con gli scopi istituzionali dell'Ateneo.

### **1.2 Scopi e applicazione**

Il presente regolamento si propone di:

- ❑ disciplinare le modalità di accesso, di utilizzo e di protezione delle risorse informatiche dell'Università degli Studi di Napoli "Parthenope";
- ❑ armonizzare l'infrastruttura ed i servizi di rete erogati dall'Ateneo, sia ad uso interno che esterno, in ogni sua struttura e funzione, comprendendone tutte le componenti hardware, software, procedurali e organizzative;

- indicare aspetti e criteri tecnici (sicurezza fisica e logica), organizzativi (definizione di ruoli, procedure e formazione) e legali per la protezione delle risorse informatiche e l'integrità dei dati;
- definire le responsabilità di quanti operano nell'ambito dell'Università ai fini del corretto utilizzo delle predette risorse;
- stabilire le sanzioni a garanzia del rispetto delle regole enunciate.

L'accesso e l'uso delle risorse informatiche dell'Ateneo comporta l'integrale ed incondizionata accettazione delle norme del presente Regolamento ed il rispetto della vigente normativa in materia. La loro non conoscenza non esime nessuno dalle proprie responsabilità.

Le regole enunciate si riferiscono a tutte le risorse informatiche dell'Università e si applicano a tutti i soggetti che le utilizzano ed alla circolazione su rete di tutte le tipologie di dati. Rimane in ogni caso inteso che:

- per le risorse informatiche messe a disposizione o date in uso all'Università da altri Enti od organizzazioni valgono gli accordi e le condizioni contrattuali stipulate fra le parti;
- per l'utilizzo di dati, programmi e materiali valgono le condizioni di copyright, ove previsto;
- l'utilizzo delle risorse informatiche dell'Università deve essere conforme a quanto previsto dalla normativa vigente.

### 1.3 Definizioni

Ai fini del presente Regolamento, si definisce come:

- a. **risorse** qualsiasi mezzo di comunicazione elettronica, sia esso hardware, software, rete, servizio ed informazione in formato elettronico di proprietà o disponibilità dell'Università o ad essa concesso in licenza d'uso.

In particolare le risorse informatiche includono:

- sistemi informativi ad uso amministrativo e/o ad uso didattico e/o scientifico e di ricerca; ogni sistema di elaborazione elettronica delle informazioni di qualsiasi livello: mainframe, mini, micro o personal computer e similari;
  - software di base e d'ambiente: sistemi operativi, software di rete, sistemi per il controllo degli accessi, package, utility e similari;
  - software applicativi: programmi in genere o mirati ai dati, fonia, sorveglianza e similari, ivi compresi quelli per il trattamento di dati ed informazioni in formato elettronico, di proprietà o comunque nella disponibilità dell'Università o ad essa concessi in licenza d'uso;
  - ogni informazione elettronica registrata o conservata in file e banche dati;
  - ogni periferica: stampanti, scanner, plotter, apparecchiature per l'archiviazione elettronica dei dati, supporti di memorizzazione, video terminali, modem, telefoni;
  - ogni dispositivo di rete di ogni tipo: centrali, centraline, concentratori, ripetitori, modem, switch, router, gateway, firewall, apparati VoIP e similari;
  - ogni mezzo trasmissivo di cablaggio strutturato per reti locali, metropolitane e geografiche: cavi in fibra e in rame per dorsali e cablaggio orizzontale, permutazioni, attestazioni, patch e similari);
- b. **rete d'Ateneo** l'insieme formato da tutte le reti locali di interconnessione delle strutture dell'Ateneo e dalle dorsali d'interconnessione tra le sue varie sedi e verso l'esterno, finalizzato a condividere le risorse informatiche comuni ed a permettere l'interscambio di informazioni e di ogni altra applicazione telematica all'interno ed all'esterno dell'Ateneo;
- c. **servizi di rete** l'insieme di tutti i servizi che, tramite la rete telematica dell'Università, è possibile ricevere o offrire all'interno e all'esterno dell'Ateneo;
- d. **dati** tutte le informazioni, indipendentemente dal formato, che sono contenute o elaborate da risorse informatiche dell'Università o che sono contenute o elaborate da risorse informatiche di altri Enti per conto dell'Università;
- e. **utente** qualsiasi soggetto, sia di ruolo e non sia a tempo indeterminato o determinato, afferente ad una qualsiasi struttura dell'Università degli Studi di Napoli "Parthenope" o di altro Ateneo

od Ente di ricerca, anche a seguito di scambi nell'ambito di programmi nazionali ed internazionali, quale, ad esempio, ogni docente, ricercatore, personale tecnico e amministrativo e studente regolarmente iscritto, nonché collaboratore, consulente o fornitore di servizi che a qualunque titolo e per il periodo di collaborazione/consulenza/convenzione, è formalmente autorizzato ad accedere ed usare le risorse disponibili ed i servizi offerti con esse per attività istituzionali dell'Ateneo. Sono definiti *utenti esterni* tutti gli altri soggetti;

- f. **responsabile della struttura** il soggetto che, indipendentemente dalla funzione organizzativa a cui presiede ed alla struttura a cui appartiene (Dipartimento, Centro, Presidenza, Laboratorio, Biblioteca e così via), ha il compito di coordinare risorse umane e tecnologiche nell'ambito di un contesto ben definito;
- g. **responsabile dei dati** il soggetto di comprovata competenza tecnica che, in relazione alle attività di servizio a cui è adibito ai vari livelli operativi (Ateneo, Facoltà, Dipartimento, Centro e così via), ha il compito di gestire dati dell'Università secondo le modalità stabilite nel presente Regolamento, nel "Regolamento sulla tutela delle persone e di altri soggetti rispetto al trattamento di dati personali" ed in collaborazione con il personale preposto del Centro di Calcolo Elettronico;
- h. **responsabile informatico**, per l'Amministrazione Centrale, il personale preposto del Centro di Calcolo Elettronico e per le strutture dipartimentali o ad esse equiparate o equiparabili, su formale richiesta, il Centro di Calcolo Elettronico ovvero soggetto della struttura o suo collaboratore di comprovata competenza tecnica che, in relazione alle attività di servizio a cui è adibito, ha il compito di gestire le risorse informatiche ivi dislocate secondo le modalità stabilite nel presente Regolamento ed in collaborazione con il personale preposto del Centro di Calcolo Elettronico;
- i. **referente informatico** qualsiasi soggetto che, in relazione alle attività di servizio a cui è adibito ai vari livelli operativi, ha l'incarico di svolgere funzioni di coordinamento tecnico fra gli utenti della struttura di appartenenza ed il personale preposto del Centro di Calcolo Elettronico relativamente all'accesso alle risorse informatiche ed all'utilizzo della rete locale, degli apparati connessi e dei servizi offerti su di essa.

## 2.0 Gestione delle risorse informatiche, della rete e dei servizi

La gestione delle summenzionate risorse, della rete e dei servizi è di competenza del personale preposto del Centro di Calcolo Elettronico dell'Università degli Studi di Napoli "Parthenope", ad esclusione delle risorse e dei servizi offerti dalle strutture dipartimentali o ad esse equiparate di competenza del Responsabile della struttura. Quest'ultimo, qualora necessario, può delegare le funzioni operative ad un suo collaboratore di comprovata competenza tecnica, nominandolo quale Responsabile dei dati e/o Responsabile informatico, tecnico ed amministrativo, con l'obbligo di mettere in pratica tutti gli accorgimenti riportati nel presente regolamento e rispondere delle eventuali inosservanze. La nomina viene accolta dagli organi competenti mediante l'emanazione del relativo decreto.

In caso la struttura non disponga di soggetto che, in base alle attività di servizio a cui è adibito ai vari livelli operativi ed alla competenza tecnica, possa aver assegnato il compito di gestire le risorse informatiche ivi dislocate, su formale richiesta, la gestione può essere demandata al Centro di Calcolo Elettronico.

Il Referente informatico, di cui alla lettera i. del precedente articolo, può coincidere con il Responsabile informatico e/o il Responsabile dei dati.

## 3.0 Security Policy

L'Università degli Studi di Napoli "Parthenope" riconosce che le informazioni gestite dai suoi sistemi informativi costituiscono una risorsa di valore strategico e che questo patrimonio deve essere efficacemente utilizzato e promosso per la crescita e lo sviluppo dell'Ateneo, nonché protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse.

Le Security Policy stabilite, comuni a tutte le strutture dell'Ateneo, si basano principalmente sulla vigente normativa in materia di sicurezza ed in particolare sui DPCM 16.01.2002, DLgs n. 196/2003, DL n. 144/2005 e loro successive integrazioni e modifiche, nonché sulle circolari e direttive CNIPA in materia di sicurezza, sulle norme che regolano la Rete Italiana dell'Università e della Ricerca Scientifica e sulle regole internazionali dell'RFC 1855.

L'Ateneo ritiene, pertanto, indispensabile assicurare l'interconnessione delle proprie strutture e con l'esterno, nonché l'adeguamento della propria infrastruttura informatica e telematica ai più recenti standard internazionali e la predisposizione di sistemi efficienti di sicurezza informatica, in modo da garantire la costante fruizione dei servizi offerti, nonché promuove lo sviluppo e diffusione di tecnologie che migliorino la sicurezza delle risorse e dei servizi, in termini di riservatezza, integrità, disponibilità e autenticità delle informazioni che transitano in rete, e di affidabilità e certificazione di chi li eroga, e si basano su infrastrutture che permettano il processo di "messa in sicurezza" delle risorse e delle attività.

Più specificamente, la gestione delle comunicazioni deve essere unica, come unica è la Rete d'Ateneo, ed insieme al trattamento dei dati personali devono essere effettuate nel rispetto delle direttive nazionali ed europee e della normativa sulla protezione dei dati personali, ogni utente deve essere identificabile e riconoscibile e la concessione dell'abilitazione all'accesso alle risorse e/o ai servizi deve avvenire solo in funzione della specificità dell'utente, la consultazione delle informazioni di carattere personale deve essere esclusivamente del legittimo proprietario, i servizi devono avere garanzia di continuità ed una chiara informativa sulle modalità di richiesta di controlli ed azioni correttive o di reclamo, i rischi di accessi non autorizzati o non consentiti e di perdita anche accidentale dei dati devono essere ridotti al minimo e le misure di protezione in relazione al progresso tecnico e all'evoluzione delle metodologie di attacco informatico devono essere individuate ed aggiornate.

Le misure minime di sicurezza stabilite comprendono:

- il monitoraggio attivo della rete, il filtraggio del traffico illegittimo, la tracciabilità delle comunicazioni telematiche e l'uso previa autenticazione dalle postazioni, specie per quelle connesse o connettabili alla rete esterna all'Ateneo;
- la protezione delle aree e dei locali, rilevanti ai fini delle comunicazioni, dei servizi e dei dati, protezione basata sul controllo fisico e logico degli accessi che per l'aspetto logico si basa su un solido sistema di autenticazione ed autorizzazione e per l'aspetto fisico va dal normale servizio di guardia e/o video-sorveglianza al controllo antieffrazione e antintrusione e sistemi per il controllo della temperatura, antincendio e di apertura delle porte d'ingresso tramite badge/smart card strettamente personali;
- una politica degli accessi alla struttura, ai server ed alle banche dati che includa un sistema di autenticazione informatica e un sistema di autorizzazione, nonché l'aggiornamento periodico dei permessi o, meglio, lo stabilire in via prioritaria chi può accedere a cosa e quando ed in che modo tale accesso debba avvenire;
- una politica di alta affidabilità e continuità dei servizi comprendente scorte di magazzino, contratti di manutenzione hardware e software, isolamento delle risorse e dei servizi critici, configurazioni ad hoc, eventuale crittografia dei dati e delle sessioni, sistema di backup centralizzato e ridondanza dei server e dei servizi e/o mirroring e/o sistemi di load balancing;
- la garanzia dell'integrità e della disponibilità delle risorse e dei servizi, a partire dalla protezione elettrica con gruppi di continuità, dal backup di server e servizi, dalla protezione delle singole postazioni, mediante password per Bios e/o sessione e/o screen-saver e/o rete, antivirus e desktop firewall, alla gestione dei supporti informatici e cartacei e ivi compresi sistemi di verifica e ripristino della disponibilità in seguito a distruzione o danneggiamento degli stessi o degli strumenti elettronici;
- l'aggiornamento periodico delle risorse e dei servizi e quindi dell'hardware, dei sistemi operativi, dei programmi, delle procedure e delle abilitazioni;

- ❑ la distribuzione formale dei compiti e delle responsabilità nell'ambito delle strutture preposte, soprattutto in merito al trattamento dei dati;
- ❑ la formazione e l'aggiornamento dei soggetti, in relazione alle attività di servizio a cui sono adibiti ai vari livelli operativi ed alle responsabilità ricevute nell'ambito delle strutture di appartenenza e/o rispetto alle risorse ed i servizi gestiti.

Le Security Policy prevedono il filtraggio del traffico tramite apparati di rete di frontiera, quali router o switch o firewall o gateway, o interni quali server proxy la cui gestione è demandata al Centro di Calcolo Elettronico. Dovranno essere filtrati almeno tutti quei collegamenti vietati dalla vigente normativa, dalla User Policy del GARR e dalle regole internazionali dell'RFC 1855 "Netiquette Guidelines", nonché quelli verso server, apparati e personal computer non offerenti servizi ufficiali e/o a valenza esterna. In casi particolari e soprattutto qualora stia per essere intaccata la garanzia dell'integrità e della disponibilità delle risorse e dei servizi, le regole adottate potranno essere più severe.

### 3.1 Login Policy

Ogni utente, per connettersi alla Rete di Ateneo, deve avere assegnato al proprio personal computer un indirizzo di rete, numerico e logico, personale e non cedibile. Il suo uso comporta l'assunzione di responsabilità riguardo le azioni dolose e colpose che possono essere con esso perpetrate: ogni attività non regolare, infrazione o abuso effettuato per suo tramite verrà imputato – nei limiti di legge – al titolare dell'indirizzo di rete.

L'indirizzo di rete va richiesto al personale preposto del Centro di Calcolo Elettronico cui è demandata la gestione del dominio e delle classi di indirizzi di rete assegnati all'Ateneo.

Gli utenti sono tenuti a seguire le indicazioni date dai referenti del Centro di Calcolo Elettronico direttamente o per tramite del Referente informatico, in merito alla configurazione e messa in rete dei propri personal computer e a non modificare tali configurazioni per alcun motivo, salvo se non espressamente richiesto dal personale preposto del Centro di Calcolo Elettronico. Ogni variazione o modifica riscontrata deve essere prontamente comunicata direttamente al Centro di Calcolo Elettronico o al Referente informatico che provvederà ad inoltrarla.

Ogni utente, per fruire delle risorse e dei servizi offerti con esse, di norma, deve avere un codice di login personale, non cedibile e costituito da una userid (codice identificazione utente) protetta da password (parola chiave ad esso abbinata) anch'essa personale, segreta, non comunicabile ad altri e per nessun motivo cedibile. L'uso di userid e password è strettamente personale e comporta l'assunzione di responsabilità riguardo le azioni dolose e colpose che tale accesso consente: ogni attività non regolare, infrazione o abuso effettuato per suo tramite verrà imputato – nei limiti di legge – al titolare del codice di login.

L'utente sprovvisto di codice di login personale, dovrà richiederne uno presso il Centro di Calcolo Elettronico direttamente o per tramite del Referente informatico, ovvero il Responsabile informatico o dei dati; la nuova password sarà attivata entro il giorno successivo. Parimenti per l'utente che dimentica la propria password.

Al primo accesso la password assegnata deve essere cambiata. La nuova password deve essere costituita da una sequenza di almeno 8 caratteri alfanumerici, non deve contenere riferimenti all'utente e non deve essere facilmente individuabile.

Gli utenti sono tenuti a conservare con diligenza la propria password ed a mantenere segrete le modalità di accesso, avendo cura che esse non vengano utilizzate in modo improprio. Gli utenti dovranno prontamente avvisare il Centro di Calcolo Elettronico ovvero il Responsabile informatico o dei dati nell'ipotesi di smarrimento del codice di login e in particolare della password, o anche solo di probabile diffusione presso terzi o se ne verificasse una rivelazione surrettizia, come in caso di rivelazione volontaria per specifici motivi.

La validità temporale del codice di login dipende dalla risoluzione del rapporto con l'Ateneo ed in particolare: per i soggetti a tempo determinato per la durata del loro contratto, per gli studenti e gli allievi annuale e rinnovabile con l'iscrizione fino al conseguimento del titolo finale, per i

soggetti a tempo indeterminato fino al pensionamento o al trasferimento presso altra Università o Ente.

La durata della password dipende dalla criticità del sistema cui si è abilitati ad accedere e, di norma, non supera l'anno solare o sei mesi, se sono coinvolti dati personali, o tre mesi se si tratta di dati sensibili e/o giudiziari. Trascorso tale periodo essa termina e va cambiata dall'utente titolare. Sarà cura dell'utente scegliere password non banali e cambiarle periodicamente. In alcun caso potrà essere confermata la vecchia password.

### **3.2 Monitoring Activity**

La normativa vigente prevede che ogni utente debba essere tracciabile ossia identificabile e riconoscibile univocamente, e le informazioni sulle attività eseguite sulla rete informatica e telematica, relative ai sistemi informatici, al traffico ed agli utenti interni ed esterni all'Ateneo, debbano essere registrate su file log e monitorate al fine di controllare il corretto utilizzo delle risorse informatiche, per la normale manutenzione dei sistemi e per attività di gestione della sicurezza, quali la protezione dell'integrità dei sistemi e dei dati in essi contenuti.

I file log, accessibili ai soli Responsabili e Addetti alla sicurezza informatica, nonché ai Responsabili delle risorse cui si riferiscono, di norma, sono conservati su supporto o apparato esterno per un periodo di ventiquattro mesi e possono essere soggetti a indagini, nel rispetto di quanto sancito dal DPCM 16.01.2002 che stabilisce i requisiti minimi per la sicurezza informatica, dal DLgs n. 196/2003 "Codice in materia di protezione dei dati personali" e dal DL n. 144/2005 sulle recenti misure anti-terrorismo e loro successive modifiche e integrazioni.

In particolare, per file contenenti dati personali e/o sensibili:

- ❑ l'accesso è consentito unicamente ad incaricati che operano sotto la diretta autorità del titolare o del Responsabile dei dati, la cui designazione è effettuata per iscritto ed individua l'ambito del trattamento consentito, oppure per i quali esiste documentata preposizione delle persone fisiche ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima;
- ❑ il trattamento è limitato a quanto è necessario per le attività di utilizzo in sicurezza delle risorse informatiche e/o per proteggere l'integrità dei sistemi informatici ed è ammesso, nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato, ove prescritti dalla vigente normativa, nonché per lo svolgimento di eventuali contestazioni anche in sede giudiziale;
- ❑ i log sono conservati per ventiquattro mesi, per finalità di accertamento e repressione dei reati e, con modalità di conservazione separata, per ulteriori ventiquattro mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici. Decorsi i termini, si provvede alla loro periodica distruzione.

L'Università tutela il diritto alla riservatezza relativo alle comunicazioni che transitano sulla Rete d'Ateneo e ai dati personali su di essa presenti, in conformità alle norme legislative e regolamentari vigenti e applicabili. Il Responsabile e gli Addetti alla sicurezza informatica dell'Ateneo possono accedere ai dati presenti sulla Rete dell'Università, anche in mancanza di consenso del titolare, nelle circostanze previste dalle norme legislative e regolamentari vigenti e applicabili.

L'utente dà atto di essere stato posto a conoscenza con il presente Regolamento del fatto che, al momento della connessione di un proprio dispositivo alla Rete d'Ateneo, il Responsabile e gli Addetti alla sicurezza informatica sono autorizzati ad utilizzare sistemi di monitoraggio della rete e dei sistemi in rete in grado di verificarne la rispondenza a quanto previsto dal presente regolamento.

### **4.0 La Rete di Ateneo ed i servizi di rete**

L'Ateneo promuove l'utilizzo della rete e dei servizi offerti per suo tramite quale strumento utile al perseguimento dei propri fini, bene comune, mezzo irrinunciabile per qualsiasi attività

istituzionale ed indispensabile al pari di altri impianti di base, demandandone la gestione al Centro di Calcolo Elettronico.

Gli utenti utilizzano liberamente la rete, usufruendo dei suoi servizi, nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme, obblighi contrattuali e delle modalità di seguito stabilite. Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, essi si impegnano ad agire con responsabilità e a non commettere abusi.

Il personale preposto del Centro di Calcolo Elettronico e/o i Responsabili informatici e/o dei dati (amministratori di sistema) installano, configurano e rimuovono componenti hardware e software e creano, modificano, rilasciano, rimuovono o utilizzano sistemi di autenticazione degli accessi per attività di gestione della sicurezza, normale manutenzione dei sistemi e protezioni dei dati, nel rispetto della vigente normativa.

Di norma, sugli elaboratori e sui personal computer con funzioni di client, devono essere garantite le seguenti condizioni:

- ❑ aggiornamento periodico del sistema operativo e del software applicativo ed ogni volta se ne riscontri l'opportunità da parte del Responsabile e degli Addetti della sicurezza informatica e/o dei Responsabili informatici e/o dei dati della struttura di appartenenza;
- ❑ disattivazione e/o disinstallazione di tutti i servizi di rete in modalità server;
- ❑ configurazione e/o pianificazione del backup delle informazioni e dei dati presenti su supporti mobili e/o su server esterni, in dipendenza della loro criticità;
- ❑ verifica del timer di sistema e sua sincronizzazione con il servizio ntp centralizzato;
- ❑ accesso univoco ossia personale e non collettivo, e non privilegiato al sistema ossia non da amministratore, con codici di login a scadenza e, se consentito dal sistema operativo, loro disattivazione automatica in caso di mancato utilizzo per un periodo superiore a 6 mesi;
- ❑ riservatezza nell'assegnazione e cambio delle password;
- ❑ assegnazione dell'indirizzo fisico e logico di rete da parte del personale preposto del Centro di Calcolo Elettronico e loro registrazione nel Domain Name Service di Ateneo;
- ❑ protezione contro virus informatici, mediante scansioni di file e della posta con idoneo antivirus;
- ❑ protezione contro intrusioni anche mediante l'uso di desktop o personal firewall.

Per gli elaboratori con funzioni di server, di norma, devono essere garantite le seguenti condizioni:

- ❑ aggiornamento periodico del sistema operativo e del software applicativo ed ogniqualvolta se ne riscontri l'opportunità da parte del Responsabile e degli Addetti della sicurezza informatica e/o del Responsabile informatico e/o dei dati della struttura di appartenenza;
- ❑ identificazione precisa dei servizi di rete e del sistema operativo offerti e la disabilitazione e/o disinstallazione dei servizi non necessari;
- ❑ configurazione e pianificazione delle procedure di backup su supporti mobili e/o su server esterni, in dipendenza della loro criticità;
- ❑ verifica del timer di sistema e sua sincronizzazione con il servizio ntp centralizzato;
- ❑ accesso privilegiato al sistema riservato al solo Responsabile (amministratore di sistema), in modalità locale o in modalità cifrata, se da remoto;
- ❑ accesso pubblico al sistema solo per i servizi di rete ufficialmente offerti;
- ❑ adozione di una adeguata e rigorosa politica di gestione delle password di accesso, con codici di login a scadenza e loro disattivazione automatica in caso di mancato utilizzo per un periodo superiore a 6 mesi, ivi compresa l'attivazione di opportuna modulistica;
- ❑ configurazione dei meccanismi di logging, in particolare per gli accessi ed i servizi;
- ❑ protezione contro virus informatici, mediante l'uso di scansioni dei file e della posta con idoneo antivirus;
- ❑ protezione fisica e logica da accessi incontrollati o non autorizzati;
- ❑ adozione di meccanismi adeguati di ripristino del sistema e di rilevazione delle intrusioni.

Su tutti gli apparati client e server ed i dispositivi di rete devono essere garantiti opportuni meccanismi e procedure di sicurezza, da concordare eventualmente con il Responsabile e gli Addetti della sicurezza informatica, adeguati alla loro funzione ed al grado di criticità dei servizi con essi offerti/fruirti, rispetto alle possibili ripercussioni sull'utenza interna ed esterna in caso di un loro eventuale malfunzionamento.

La mancata applicazione anche di parte delle summenzionate condizioni e/o la loro successiva variazione non autorizzata o non concordata, può comportare la revoca delle autorizzazioni del client o del server, e quindi la non fruibilità o visibilità dei servizi.

I Responsabili delle strutture ovvero i Responsabili dei dati e/o i Responsabili informatici da loro delegati, forniscono al Responsabile ed agli Addetti della sicurezza informatica tutte le informazioni relative all'organizzazione dei servizi erogati dalla struttura da loro diretta. Tali dati, in forma anonima nei casi previsti dalla vigente normativa, potranno essere forniti al Comitato per la sicurezza informatica per lo svolgimento di quanto ad esso demandato.

Il Responsabile e gli Addetti all'implementazione e alle verifiche della sicurezza informatica dovranno provvedere al controllo delle misure di protezione adottate, in accordo con le indicazioni riportate nel presente Regolamento, valutandole e prospettando eventuali interventi ed ogni altra iniziativa che riterranno necessaria per la salvaguardia della risorsa e/o servizio considerato e delle relative informazioni.

#### **4.1 La Rete di Ateneo**

La Rete è l'infrastruttura costituita dal cablaggio passivo - cavi in rame, fibre ottiche e altri mezzi trasmissivi - e attivo - switch, router e apparati di rete in genere - che permette lo scambio di informazioni e l'accesso ai servizi di rete internamente ed esternamente all'Ateneo.

La politica e la gestione del routing ossia dell'instradamento delle informazioni su rete ed il monitoraggio della rete, ivi comprese le loro modifiche per l'implementazione di nuove tecnologie e/o servizi, sono di competenza esclusiva del Centro di Calcolo Elettronico, così come sono ad esso demandate le funzioni di sviluppo, pianificazione, aggiornamento, gestione, controllo e manutenzione dell'infrastruttura di rete, sotto l'aspetto fisico/logico e curandone i relativi progetti fino alla presa utente compresa, nonché quanto necessario per il collegamento con le realtà nazionali e internazionali.

La responsabilità amministrativa e tecnica per gli apparati a valle della presa utente sono di competenza del personale preposto del Centro di Calcolo Elettronico ovvero dei Responsabili delle strutture e/o dei Responsabili informatici ove presenti.

In particolare, il Centro di Calcolo Elettronico assicura la connessione di ogni struttura dell'Ateneo, presso le sedi esistenti e quelle di nuovo allestimento:

- ❑ pianificando i collegamenti e le bande trasmissive in base alle esigenze e le richieste pervenute, nonché alle disponibilità finanziarie dell'Amministrazione;
- ❑ curando la progettazione del cablaggio per la realizzazione e l'adeguamento della Rete di Ateneo ovvero di sue tratte o rami;
- ❑ gestendo i domini e gli indirizzi di rete pubblici assegnati all'Ateneo;
- ❑ gestendo il routing, il filtering ed il firewalling del traffico sulla Rete d'Ateneo;
- ❑ armonizzando le risorse, il loro utilizzo e gestione, nonché il controllo degli accessi;
- ❑ curando accordi specifici tra l'Ateneo e la Rete Italiana dell'Università e della Ricerca Scientifica, denominata comunemente "Rete GARR", e/o gli Enti interessati (convenzioni o atti aggiuntivi a convenzioni già esistenti) in collaborazione con i rispettivi responsabili degli Enti stessi.

Fin dalle fasi di predisposizione di nuove sedi o ristrutturazioni, il personale preposto del Centro di Calcolo Elettronico provvede alle opere di cablaggio ed alle relative apparecchiature per l'estensione del Rete d'Ateneo alla nuova sede, proponendo il risultato agli organi competenti per l'approvazione ed il relativo finanziamento e seguendone la successiva messa in opera/funzione. Tale cablaggio dovrà rispettare le norme nazionali e internazionali, pianificando i collegamenti e le

bande trasmissive e stabilendo, qualora fosse necessario, delle bande massime di utilizzo verso i collegamenti metropolitani, regionali, nazionali ed internazionali.

Dove esistano impianti obsoleti che influiscano negativamente sulla rete o nel caso in cui una tratta o un ramo diventi insufficiente alle necessità di coloro che ne fruiscono, il summenzionato personale del Centro di Calcolo Elettronico ne proporrà l'adeguamento agli organi competenti dell'Amministrazione e ne seguirà la messa in opera.

La Rete dell'Ateneo è realizzata rispettando gli standard internazionali inerenti il cablaggio strutturato, l'architettura più innovativa e la scalabilità degli apparati: ogni edificio/sede ha un locale centro stella che lo collega agli altri edifici/sedi tramite link in fibra ottica costituenti le "dorsali di campus"; dai singoli locali centro stella partono cavi in fibra ottica, le "dorsali di edificio", diretti ai vari locali tecnici presenti sui diversi piani, dove è situata la parte attiva del cablaggio: gli apparati di rete; dai locali tecnici si dirama infine la distribuzione orizzontale di piano, di norma in rame, verso le singole prese utente. Tali prese costituiscono i punti terminali di connessione fonia/dati ai quali possono essere collegati vari "sistemi terminali di rete" quali personal computer, terminali, stampanti, telefoni, fax o periferiche in genere.

Gli apparati di rete, come modem, hub, switch e router, non sono considerati "sistemi terminali di rete" ed il loro uso deve essere preventivamente autorizzato e concordato con il personale preposto del Centro di Calcolo Elettronico.

Qualora le esigenze di connessione alla rete nazionale ed internazionale lo richiedessero, il summenzionato personale provvederà alla realizzazione di un piano di migrazione, proponendolo agli organi competenti per l'approvazione ed il relativo eventuale finanziamento e seguendone la successiva messa in opera/funzione. Tale piano di migrazione dovrà comprendere le tempistiche, i problemi tecnici, gli aspetti economici e tutto quanto sia necessario per adeguare il preesistente e poter mantenere la connettività verso l'esterno.

La tecnologia utilizzata per l'implementazione della sicurezza di rete è incentrata prevalentemente su di un sistema distribuito di VLAN (Virtual Local Area Network) e di firewalling con architettura screened host/port e filtri alle richieste esterne di connessione, realizzato da packet filtering sugli apparati di bordo ed integrato da proxy server e da altri apparati nell'Intranet. Sono, di norma, filtrate le connessioni di cui all'ultimo comma dell'art. 3.0 e quelle in ingresso verso i server dell'Ateneo: transita solo il traffico legittimo ossia quello verso i servizi ufficiali dell'Ateneo.

Ogni utente può accedere a tutti servizi offerti per suo tramite, nel rispetto della vigente normativa, delle norme del GARR, delle regole internazionali dell'RFC 1855 e del presente Regolamento. In ogni caso le informazioni relative alle connessioni da e verso la Rete di Ateneo (orario, durata e tipo della connessione, mittente e destinatario) vengono registrate in file di log e rese disponibili secondo le modalità descritte nel presente Regolamento.

Il personale preposto del Centro di Calcolo Elettronico è tenuto ad osservare e far osservare non solo le norme nazionali ed internazionali, ma anche quelle relative alle iniziative metropolitane, regionali e di ogni altro tipo a cui l'Ateneo partecipa, nonché alla loro divulgazione anche mediante la pubblicazione sul sito Web dell'Ateneo.

## **4.2 Servizi di rete**

I servizi di rete sono un bene comune dell'Ateneo, uno strumento di lavoro e di promozione delle attività didattiche, amministrative, scientifiche e di ricerca dell'Università. Di norma, sono offerti centralmente, ma possono essere erogati anche in modo distribuito, lasciando spazi di autonomia alle singole strutture erogatrici, purché tali iniziative siano armonizzate alle regole comuni e con una precisa individuazione di ruoli e relative assunzioni di responsabilità.

I servizi di rete, erogati con le modalità nel seguito indicate, si distinguono in:

- ❑ servizi per Intranet, offerti ed accessibili esclusivamente a tutti gli utenti interni;
- ❑ servizi per Internet, offerti ed accessibili a tutti gli utenti interni e, per i soli server autorizzati, a tutti gli utenti esterni.

I servizi erogati per l'Intranet non sono visibili all'esterno della Rete di Ateneo.

Il Centro di Calcolo Elettronico, cui è demandata la gestione delle risorse e dei servizi di rete dell'Ateneo, è il referente per i servizi classici, quali la risoluzione dei nomi del dominio (DNS) e la posta elettronica, per i servizi fruibili via Web e per quelli avanzati come il VoIP e la didattica a distanza, nonché per lo studio e lo sviluppo di nuovi servizi da offrire su rete.

Ogni struttura che voglia erogare un servizio di rete visibile dall'esterno, deve non solo garantire il rispetto delle norme di sicurezza indicate dal presente Regolamento, ma deve anche avere la necessaria autorizzazione affinché le regole di filtro implementate consentano il transito di pacchetti destinati al servizio. In caso contrario il servizio di rete non è accessibile dall'esterno.

L'implementazione della sicurezza dei servizi di rete e le tecnologie utilizzate nei vari servizi, si basano essenzialmente su quanto stabilito all'art. 3.0 e seguenti del presente Regolamento. Per i servizi considerati critici, come ad esempio la rete e/o la fonia e/o la posta elettronica e/o i servizi web, sono implementate ulteriori misure al fine di garantire maggiormente la loro continuità ed affidabilità, anche mediante la previsione tecnica ed economica di meccanismi di reperibilità dei responsabili in casi ove necessita un tempestivo intervento.

#### **4.3 Dominio ed indirizzi di rete**

Il dominio di secondo livello assegnato all'Università degli Studi di Napoli "Parthenope" dalle autorità nazionali ed internazionali è "uniparthenope.it". Tale dominio appartiene esclusivamente all'Ateneo che con esso viene riconosciuto a livello nazionale ed internazionale.

Sotto tale dominio sono utilizzati più spazi di indirizzamento IP: le reti pubbliche di classe C 192.167.9.0 e 193.205.230.0, assegnate all'Ateneo dalle competenti autorità per la fruizione/l'offerta di servizi ed i collegamenti da e verso l'esterno, e reti private per la fruizione/l'offerta di servizi ed i collegamenti all'interno dell'Ateneo. Un qualsiasi indirizzo di rete, numerico o logico, appartenente al dominio dell'Università è di sua proprietà e viene assegnato all'utente per lo svolgimento di attività istituzionali nell'ambito delle proprie funzioni e/o competenze; ne consegue che in alcun caso esso può essere considerato dato personale.

L'organizzazione dei domini e degli indirizzi di rete nazionali ed internazionali ha una struttura gerarchica ad albero rovesciato e, conseguentemente, è tale anche quella dell'Ateneo. Il Presidente del Centro di Calcolo Elettronico assume la responsabilità amministrativa del dominio e dello spazio di indirizzamento IP, assegnati all'Ateneo dalle competenti autorità nazionali ed internazionali, ed il personale preposto del Centro di Calcolo Elettronico assegna gli indirizzi ai server, ai personal computer ed ai dispositivi degli utenti che se ne assumono la piena responsabilità d'uso, e ne concorda i nomi logici con essi e/o i Responsabili e/o i Referenti informatici delle strutture.

È compito del summenzionato personale preposto garantire in ogni momento il corretto funzionamento del dominio e dei suoi servizi di risoluzione degli indirizzi, di alias e così via, in modo che ogni apparato connesso alla Rete d'Ateneo abbia un indirizzo di rete pubblico o privato, in dipendenza delle funzioni cui è destinato, ed un corrispondente nome logico di dominio univoco, statico e registrato nel Domain Name System ufficiale dell'Ateneo, in ottemperanza della vigente normativa in tema di autenticazione e tracciabilità delle comunicazioni.

La continuità, l'affidabilità e la sicurezza della gestione del dominio e dei suoi servizi dovranno essere garantite da idonee misure basate sulla ridondanza delle risorse, anche in base alle funzioni cui sono dedicati gli apparati, su idonee politiche di autenticazione/autorizzazione delle richieste e dei richiedenti ed anche mediante la previsione tecnica ed economica di meccanismi di reperibilità dei responsabili in casi ove necessita un tempestivo intervento.

Qualora le esigenze dell'Ateneo e/o gli organismi nazionali ed internazionali lo richiedessero, il personale preposto del Centro di Calcolo Elettronico provvederà alla realizzazione di piani di migrazione proponendoli agli organi competenti per l'approvazione ed il relativo eventuale finanziamento e seguendone la successiva messa in opera/funzione. Tali piani dovranno

comprendere le tempistiche, i problemi tecnici, gli aspetti economici e tutto quanto sia necessario per adeguare il preesistente, in garanzia della loro continuità ed affidabilità.

#### 4.4 Posta elettronica

La posta elettronica ossia la trasmissione di tutti i tipi di informazioni, documenti e comunicazioni in formato elettronico, a differenza di altri mezzi tradizionali, offre notevoli vantaggi in termini di:

- ❑ maggiore semplicità ed economicità di trasmissione, inoltro e riproduzione;
- ❑ semplicità ed economicità di archiviazione e ricerca;
- ❑ facilità di invio multiplo con costi estremamente più bassi di quelli dei mezzi tradizionali;
- ❑ velocità ed asincronia della comunicazione, in quanto non richiede la contemporanea presenza degli interlocutori;
- ❑ possibilità di consultazione ed uso anche da postazioni diverse da quella del proprio ufficio, anche al di fuori della sede ed in qualunque momento, grazie alla persistenza del messaggio nella sua casella di posta elettronica;
- ❑ integrabilità con altri strumenti di automazione di ufficio, quali rubrica, agenda, lista di distribuzione ed applicazioni informatiche in genere.

L'Università degli Studi di Napoli "Parthenope", ferma restando l'osservanza delle norme in materia della riservatezza dei dati personali e delle norme tecniche di sicurezza informatica, in ottemperanza ai più recenti dettami normativi, si adopera per estendere l'utilizzo la posta elettronica al suo interno assegnando a tutti i dipendenti una casella di posta elettronica (anche quelli per i quali non sia prevista la dotazione di un personal computer) ed attivando apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza. Queste ultime dovranno procedere alla tempestiva lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta, adottando gli opportuni metodi di conservazione della stessa in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.

I server ufficiali di posta elettronica dell'Ateneo sono gli unici visibili all'esterno della Rete d'Ateneo e sono curati dal personale preposto del Centro di Calcolo Elettronico che ne assicura in modo esclusivo la gestione, il monitoraggio, la sicurezza, l'aggiornamento e la pubblicizzazione secondo le regole definite nel presente Regolamento. Essi hanno adeguati meccanismi di sicurezza, in rispetto della vigente normativa nazionale ed internazionale, e sono configurati in modo da assicurare l'affidabilità e la continuità del servizio e da non recare danni alle attività di altri utenti o servizi disponibili sulla rete. In particolare, sono attivati sistemi antivirus e anti-spamming a monte del servizio ed è evitato il mail-relay verso host esterni alla rete.

La continuità, l'affidabilità e la sicurezza della gestione del servizio di posta elettronica dovranno essere garantite da idonee misure basate sulla ridondanza delle risorse e/o sistemi di mirroring o load balancing, anche in base alle funzioni cui sono dedicati gli apparati, su idonee politiche di autenticazione/autorizzazione delle richieste e dei richiedenti ed anche mediante la previsione tecnica ed economica di meccanismi di reperibilità dei responsabili, in casi ove necessita un tempestivo intervento.

Ogni messaggio di posta elettronica viene considerato dato personale ed è pertanto vietata ogni sua intercettazione non autorizzata, fatte salve esigenze specifiche di monitoraggio e sicurezza in base alla normativa vigente.

La trasmissione non cifrata di informazioni personali o sensibili a mezzo di posta elettronica è subordinata all'accettazione da parte del mittente della loro vulnerabilità.

La trasmissione di informazioni riservate mediante posta elettronica è subordinata all'approvazione del Responsabile della struttura.

In ottemperanza alla normativa vigente, dovrà essere attivato il servizio di posta certificata secondo il quale l'accesso alle caselle ufficiali di posta elettronica dovrà gradualmente migrare verso protocolli in modalità cifrata come SPOP o SIMAP, le comunicazioni ufficiali dell'Ateneo dovranno essere autenticate con sistemi di certificazione interni a chiave asimmetrica, gestiti dal

Responsabile e dagli Addetti alla sicurezza informatica dell'Ateneo, e la lettura di tali messaggi potrà essere certificata solo con software che prevedano tale modalità come i mail agent di Netscape ed Explorer Messenger.

Qualora le esigenze dell'Ateneo e/o nuove tecnologie e/o gli organismi nazionali ed internazionali lo richiedessero, il personale preposto del Centro di Calcolo Elettronico e/o il Responsabile e gli Addetti della sicurezza informatica provvederanno alla realizzazione di piani di migrazione proponendoli agli organi competenti per l'approvazione ed il relativo eventuale finanziamento e seguendone la successiva messa in opera/funzione. Tali piani dovranno comprendere le tempistiche, i problemi tecnici, gli aspetti economici e tutto quanto sia necessario per adeguare il preesistente, in garanzia della continuità ed affidabilità del servizio.

#### **4.5 Fonia**

Il sistema di fonia dell'Università, facente capo alla radice passante 081 5474/5/6, è costituito da un centro stella dislocato nella sede centrale dell'Ateneo, comprendente una centrale telefonica Ericsson MD110, sistema di gestione via rete telematica ed apparati centralizzati per il sistema addebiti, e quattro centri periferici in sedi metropolitane e dell'interland campano, anch'esse di simile composizione.

Le chiamate in uscita ed in ingresso vengono assicurate da collegamenti ISDN primari, per la sede centrale, e dalle dorsali di campus della Rete d'Ateneo per le sedi di maggior dimensione o fasci di ISDN opportunamente dimensionati per le restanti sedi, sulla base di uno schema di bilanciamento ottimizzato in base al traffico. Per il sistema centrale ed almeno per le sedi di maggior dimensione sono presenti collegamenti di backup al fine di assicurare la continuità del servizio.

Per la distribuzione negli edifici, di norma, utilizza il cablaggio strutturato realizzato per la Rete d'Ateneo e, pertanto, ne assume le definizioni e le norme previste dall'art. 4.3 del presente Regolamento. La distribuzione è basata su collegamenti di tipo analogico e digitale, la cui gestione tecnica è demandata al personale preposto del Centro di Calcolo Elettronico per garantire la centralità di gestione del sistema di fonia di Ateneo, e sui relativi apparecchi telefonici forniti dall'Amministrazione dell'Ateneo per garantirne la piena compatibilità con il sistema.

Data la criticità del servizio, il summenzionato personale preposto ne assicura in modo esclusivo la gestione, il monitoraggio, la sicurezza, l'aggiornamento e la pubblicizzazione secondo le regole definite dal presente Regolamento ed anche mediante la previsione tecnica ed economica di meccanismi di reperibilità dei responsabili, in casi ove necessita un tempestivo intervento.

È in atto la sperimentazione del servizio VoIP, Voice over IP, evoluzione del classico servizio di fonia verso servizi di comunicazione avanzata, fruibili tramite "multiservice network" infrastrutture di trasporto integrato ad alta velocità, al cui termine è prevista la graduale migrazione dalla fonia tradizionale verso il nuovo servizio. Non saranno, pertanto, fornite di centro stella tradizionale per la fonia le sedi di nuova acquisizione, costruzione e/o allestimento.

La tecnologia utilizzata per l'implementazione della sicurezza del servizio di fonia è incentrata sulla separazione fisico/logica delle trasmissioni e del traffico: le dorsali di campus sono provviste di canali ad esso dedicati, le terminazioni di tali dorsali sono su apparati esclusivamente rivolti al servizio e la distribuzione negli edifici avviene con idonea permutazione a livello dei locali tecnici, per la fonia tradizionale, e mediante l'utilizzo di indirizzi di rete privati dedicati e di VLAN (Virtual Local Area Network).

#### **4.6 Siti e servizi web**

I siti web pubblici dell'Università degli Studi di Napoli "Parthenope" e delle sue strutture didattiche e di ricerca, rivestono un ruolo di primaria importanza, soprattutto in merito alla visibilità dell'Ateneo e delle sue strutture, e divengono oltremodo vitali per la diffusione delle informazioni didattiche, amministrative e scientifiche e la trasparenza degli atti verso gli utenti interni ed esterni.

Prevedendone la naturale evoluzione verso livelli di sempre maggiore interattività con l'utenza, essi sono funzionalmente classificati secondo due tipologie:

- **siti di informazione**, non connessi con i sistemi informativi e le banche dati dell'Ateneo e destinati al dialogo con l'utenza interna e/o esterna mediante dati, notizie, informazioni la cui conoscenza può avere interesse o utilità per chi vi accede, e caratterizzati da un flusso informativo monodirezionale dall'Ateneo verso l'utente;
- **siti di servizio**, connessi con i sistemi informativi e le banche dati dell'Ateneo, che permettono all'utente interno e/o esterno di intrattenere rapporti ufficiali con singole strutture dell'Ateneo, di interagire con esse e di ottemperare ad adempimenti didattici, amministrativi e normativi.

In entrambe i casi, vanno garantite la continuità e l'affidabilità del servizio, nonché le funzionalità di sicurezza, integrità e riservatezza delle informazioni pubblicate e/o trattate, tramite idonee misure basate sulla ridondanza delle risorse e/o sistemi di backup e mirroring o load balancing, in base alle funzioni cui sono dedicati gli apparati, su idonee politiche di autenticazione/autorizzazione delle richieste e dei richiedenti ed anche mediante la previsione tecnica ed economica di meccanismi di reperibilità dei responsabili, in casi ove necessita un tempestivo intervento.

La vigente normativa riconosce la centralità e l'importanza delle informazioni pubblicate con tale servizio, stabilendo misure per l'accessibilità e l'usabilità dei siti web poiché un sito accessibile a tutti è un ingresso preferenziale al patrimonio di informazioni e di servizi offerto e rende sempre più fruibile questo patrimonio, diffondendo l'offerta e permettendone a chiunque la fruizione anche se con modalità e strumenti di accesso differenziati. Rendere un sito accessibile significa, quindi, permettere a chiunque di accedere alle pagine, consultarle, usufruire dei servizi e delle informazioni indipendentemente dal sistema operativo, dagli strumenti di navigazione, dalle impostazioni del browser ed a prescindere dalla velocità di connessione di cui si dispone.

L'Ateneo, aderendo in pieno alla normativa sull'accessibilità e usabilità dei siti web e ritenendo fondamentale per gli scopi istituzionali la sua applicazione, dispone per i suoi siti ufficiali l'applicazione delle quattordici linee guida indicate dal W3C, World Wide Web Consortium, che possono essere così sintetizzate:

- Fornire alternative equivalenti per il contenuto visivo e audio, un contenuto che, presentato all'utente, svolga la stessa funzione o raggiunga lo stesso scopo del contenuto visivo o acustico.
- Non fare affidamento unicamente sul colore, ma assicurarsi che il testo e la parte grafica siano comprensibili anche se consultati senza di esso.
- Usare in maniera appropriata marcatori, preferendo gli appositi elementi strutturali, e fogli di stile piuttosto che elementi e attributi di presentazione.
- Rendere chiaro l'uso del linguaggio naturale utilizzando marcatori che agevolino la pronuncia o l'interpretazione di testi in lingua straniera od anche abbreviazioni e acronimi.
- Creare tabelle che si trasformino in maniera elegante ossia che siano interpretate e trasformate correttamente dai browser e dagli altri user agent.
- Garantire che le pagine che utilizzano le tecnologie più recenti siano interpretate correttamente e rimangano accessibili anche quando le tecnologie più recenti non sono supportate o sono disattivate.
- Garantire all'utente il controllo dei mutamenti di contenuto dipendenti dal tempo ossia che il movimento, il lampeggiare, lo scorrere e l'aggiornamento automatico di oggetti possa essere messo in pausa o arrestato.
- Assicurarsi che l'interfaccia utente incorporata sia conforme ai principi di progettazione accessibile: accesso alle funzionalità indipendente dal dispositivo, possibilità di operare da tastiera, comandi vocali, etc.
- Progettare garantendo l'indipendenza dal dispositivo, usando funzioni che permettano di attivare gli elementi della pagina mediante una varietà di dispositivi.
- Usare soluzioni temporanee per l'accessibilità, affinché le tecnologie assistive e i browser più vecchi possano operare correttamente.

- ❑ Usare le tecnologie (in conformità con le specifiche) e le linee guida per l'accessibilità del W3C o fornire una versione alternativa accessibile del contenuto.
- ❑ Fornire informazioni di contesto e orientamento per aiutare gli utenti a comprendere pagine o elementi complessi.
- ❑ Fornire meccanismi di navigazione chiari e consistenti - informazioni di orientamento, barre di navigazione, una mappa del sito, etc. - per aumentare la probabilità che una persona possa trovare sul sito ciò che sta cercando.
- ❑ Garantire che i documenti siano chiari e semplici, affinché possano essere più facilmente comprensibili.

Il Centro di Calcolo Elettronico si occupa della gestione del sito e dei servizi web d'Ateneo, del coordinamento dei siti web ufficiali e del rispetto della vigente normativa in materia, nonché della gestione dei siti e dei servizi web su richiesta delle relative strutture dell'Ateneo, garantendo la solidità hardware e software, la gestione centralizzata dei server, la sicurezza degli accessi differenziati e, nel contempo, la standardizzazione degli applicativi utilizzati per script e database, nonché l'unicità delle banche dati, onde evitare inutili duplicazioni o diverso stato di aggiornamento dei dati e favorire la sicurezza, integrità e riservatezza del loro trattamento.

I servizi web possono essere erogati anche in modo distribuito, lasciando spazi di autonomia alle singole strutture didattiche, di servizi e di ricerca erogatrici, purché tali iniziative siano armonizzate alle regole comuni, alle scelte editoriali e di pubblicazione delle informazioni espresse dall'Ateneo, e con una precisa individuazione di ruoli e relative assunzioni di responsabilità.

Ogni struttura che voglia erogare un servizio web visibile dall'esterno, deve non solo garantire il rispetto delle norme indicate dal presente Regolamento, ma deve anche avere la necessaria autorizzazione affinché le regole di filtro implementate consentano il transito di pacchetti destinati al servizio. In caso contrario il servizio non è accessibile dall'esterno.

#### **4.7 Servizi tradizionali, elettronici, nuovi ed avanzati**

Tutti i servizi tradizionali, nuovi ed avanzati erogati e promossi dall'Università degli Studi di Napoli "Parthenope" ed in modo distribuito dalle sue strutture didattiche, di servizi e di ricerca, devono essere armonizzati alle regole comuni del presente Regolamento e alle scelte espresse dall'Ateneo e, specie se diretti anche all'utenza esterna, con una precisa individuazione di ruoli e relative assunzioni di responsabilità.

Le strutture o gli utenti che intendono attivare servizi sulla Rete d'Ateneo non destinati alle attività didattiche, di ricerca o comunque istituzionali, come bollettini, fogli redazionali o testate giornalistiche quali bacheche elettroniche, giornali elettronici ed altri strumenti assimilabili, allo scopo di manifestare liberamente il loro pensiero nel rispetto dei diritti degli altri utenti e dei terzi, devono richiedere l'autorizzazione al Rettore, previo parere della struttura competente.

Essi si devono impegnare a comportarsi in modo corretto, responsabile e conforme alle norme vigenti, e devono dichiarare per iscritto che intendono assumersi la responsabilità degli abusi che possono essere commessi, anche da terzi, attraverso detti servizi.

In presenza di tali condizioni, il Rettore autorizza l'attivazione di tali servizi.

Ciascun utente può in ogni momento ricorrere al Rettore per far accertare la legittimità dell'attività svolta attraverso tali servizi e la conformità della stessa al presente Regolamento e alle normative vigenti.

In ogni caso, vanno garantite la continuità e l'affidabilità del servizio, nonché le funzionalità di sicurezza, integrità e riservatezza delle informazioni trattate, nel rispetto di quanto esposto dalla normativa vigente, dalle regole nazionale ed internazionali e dal presente Regolamento, e tramite idonee misure basate almeno su efficaci sistemi di backup, su idonee politiche di autenticazione/autorizzazione delle richieste e dei richiedenti, nonché la previsione tecnica ed economica di meccanismi di reperibilità dei responsabili, in casi ove necessita un tempestivo intervento.

Per i servizi considerati critici potrà essere emanato apposito regolamento che preveda regole più particolareggiate, non solo per la sua fruizione, ma soprattutto in materia di sicurezza, per la gestione degli incidenti e le conseguenti modalità di intervento e ripristino.

#### 4.8 Dati e informazioni

Qualsiasi dato o informazione, ivi compresa la disposizione logica dei dati stessi, sia esso inerente alla didattica, alla ricerca o alle attività scientifica ed amministrativa, è un bene dell'Università degli Studi di Napoli "Parthenope" e deve essere pertanto protetto da distruzioni o perdite anche accidentali, alterazioni, usi illeciti e divulgazioni non autorizzate.

La tutela delle persone e di altri soggetti rispetto al trattamento di dati personali e per l'adozione di misure minime di sicurezza è oggetto di apposito regolamento in via di emanazione, tuttavia, si definiscono, per gli scopi del presente Regolamento:

- ❑ **titolare dei dati:** raccolti o meno in banche di dati, automatizzate o cartacee, è l'Università degli Studi di Napoli "Parthenope", nella persona del Rettore;
- ❑ **banca dati:** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- ❑ **trattamento:** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- ❑ **responsabile:** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali che per le strutture amministrative e di servizio dell'Ateneo sono individuabili nei dirigenti/funzionari responsabili delle strutture stesse, mentre per le strutture didattiche e di ricerca, sono individuabili nei direttori delle strutture stesse;
- ❑ **incaricati:** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile dei dati;
- ❑ **dati comuni:** le informazioni riguardanti l'attività didattica, di servizio, scientifica e di ricerca dell'Ateneo;
- ❑ **dati amministrativi:** le informazioni e le comunicazioni riguardanti l'amministrazione dell'Ateneo per il conseguimento dei propri fini istituzionali, ivi compresi quelli riservati ossia ad uso interno o coperti dal segreto d'ufficio;
- ❑ **dati personali:** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- ❑ **dati sensibili:** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché quelli idonei a rivelare lo stato di salute e la vita sessuale;
- ❑ **dati giudiziari:** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- ❑ **dati critici:** le informazioni, le applicazioni informatiche o i sistemi operativi relativi agli host fornitori di servizi di rete ed a quelli che possono compromettere significativamente la sicurezza della rete di Ateneo;
- ❑ **dati anonimi:** i dati che in origine o a seguito di trattamento, non possono essere associati ad un interessato identificato o identificabile;

- ❑ **misure minime:** il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del D.Lgs. 196/2003.

Il Titolare dei dati, con proprio provvedimento, può designare responsabili del trattamento dei dati altri soggetti, anche esterni all'Ateneo, cui affidare l'espletamento di attività strumentali. Nel caso di stipula di contratti o di convenzioni la cui esecuzione implichi la conoscenza anche eventuale di dati personali di cui l'Università è titolare, il contraente deve essere nominato, con atto del Rettore, responsabile del trattamento dei dati medesimi.

All'interno delle singole strutture di diretta responsabilità, i Responsabili dei trattamenti procedono con propri atti scritti comunicati in modo formale all'Amministrazione ed in coordinamento con essa, all'individuazione nominativa degli incaricati del trattamento dei dati personali, cui spetta il compito di svolgere le operazioni materiali inerenti al trattamento dei dati stessi operando sotto la diretta responsabilità del Responsabile.

Il Responsabile del trattamento che ne intraprende un nuovo o cessa uno già esistente, è tenuto a comunicarlo all'Amministrazione in via ordinaria, nonché al Responsabile della sicurezza informatica se per il trattamento è necessaria l'attuazione e/o l'adozione di misure di sicurezza.

Nella comunicazione dovranno essere indicate:

- ❑ le finalità e le modalità del trattamento;
- ❑ il nome del responsabile del trattamento;
- ❑ la natura dei dati, il luogo ove essi sono custoditi e le categorie di interessati cui i dati si riferiscono nonché la lista nominativa dei responsabili e degli incaricati del trattamento autorizzati ad operare sui dati medesimi;
- ❑ l'ambito di comunicazione e di diffusione dei dati ossia il darne conoscenza ad uno o più soggetti, rispettivamente determinati e indeterminati, diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- ❑ gli eventuali trasferimenti di dati previsti verso Paesi non appartenenti all'Unione Europea o, qualora si tratti di dati sensibili e di dati relativi ai provvedimenti di cui all'art. 686 c.p.p., fuori dal territorio nazionale;
- ❑ una descrizione delle misure di sicurezza adottate;
- ❑ l'eventuale connessione con altri trattamenti o banche di dati;
- ❑ le eventuali modalità tecniche di accesso ai dati all'interno (Intranet) ed dall'esterno (Internet) della Rete di Ateneo.

I dati personali oggetto di trattamento sono raccolti, conservati e trattati secondo le modalità e con i requisiti previsti dal D.Lgs n. 196/2003 e successive modifiche ed integrazioni.

All'interessato, i cui dati sono contenuti in una banca di dati dell'Università degli Studi di Napoli "Parthenope", spettano i diritti di cui a titolo II del D.Lgs n. 196/2003 e successive modifiche ed integrazioni.

Ogni singola struttura dell'Università provvederà ad assolvere agli obblighi di informativa imposti nei confronti dell'interessato ogni qualvolta si provveda alla raccolta dei dati personali, esplicitando, oralmente o cartaceamente o elettronicamente, prima della raccolta:

- ❑ le finalità e le modalità del trattamento cui sono destinati i dati;
- ❑ la natura obbligatoria o facoltativa del conferimento dei dati;
- ❑ le conseguenze di un eventuale rifiuto di rispondere;
- ❑ i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei medesimi;
- ❑ i diritti riconosciuti all'interessato;
- ❑ il nome, la denominazione o la ragione sociale ed il domicilio, la residenza o la sede del titolare e del responsabile del trattamento dei dati.

L'implementazione della sicurezza dei dati informatizzati, organizzati o meno in banche dati, è a cura dei rispettivi Responsabili dei dati e del trattamento che, coadiuvati dal Responsabile e dagli Addetti della sicurezza informatica dell'Ateneo, assicurano l'adozione di idonee misure di

sicurezza e garantiscono la protezione degli accessi e l'integrità degli archivi. Essi custodiscono i dati, adottando misure idonee ad evitare i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato, e di trattamento non consentito o non conforme allo scopo della raccolta.

#### 4.9 Formazione

L'Ateneo ritiene che l'istruzione degli utenti e la formazione permanente del personale sia lo strumento principale per l'utilizzo efficiente, corretto e sicuro delle risorse informatiche e della rete e dei servizi di rete, e, pertanto, adotta ogni iniziativa di sostegno e di formazione per promuoverne l'uso da parte di tutto il personale.

In particolare, saranno promosse iniziative volte al supporto degli utenti, nei vari momenti di uso delle risorse e fruizione dei servizi, a partire da semplici users guide, mailing list e news fino alla realizzazione di minicorsi con sistemi di eLearning. Il piano di formazione del personale sarà adeguato sia tecnicamente che economicamente, prevedendo una differenziazione in relazione alle attività di servizio a cui esso è adibito ai vari livelli operativi ed un'articolazione in moduli teorico-pratici, per avviare e monitorare il processo di evoluzione delle competenze manageriali e professionali atte a renderle più rispondenti e coerenti con le nuove esigenze di fruizione delle risorse ed offerta dei servizi informatici. L'aggiornamento professionale, ottenuto anche mediante la realizzazione di piattaforme di eLearning, dovrà essere integrato da interventi pianificati di comunicazione, volti a migliorare il coinvolgimento e la sensibilizzazione del personale ed a promuovere l'adesione e l'uso delle risorse informatiche riferite agli obiettivi da raggiungere.

#### 5.0 Accesso ed uso delle risorse informatiche e dei servizi

Le risorse informatiche dell'Università devono essere utilizzate esclusivamente per l'assolvimento delle finalità proprie dell'Ateneo ossia per attività didattiche, di ricerca, scientifiche ed amministrative.

Le modalità di accesso variano, a seconda delle tipologie dei soggetti e dei servizi, sulla base di criteri organizzativi e tecnici individuati dal Centro di Calcolo Elettronico ovvero dai Responsabili informatici e/o dei dati, e pubblicati anche sui siti web d'Ateneo.

È fatto obbligo a tutti gli utenti di prendere atto e rispettare ogni altra norma, istruzione o dettaglio tecnico pubblicati sulle apposite pagine dei siti web dell'Ateneo che il personale preposto ovvero i Responsabili informatici e/o dei dati dovranno farsi carico di tenere aggiornate, evidenziandone le novità anche mediante l'invio e/o utilizzo di news, mailing list o qualsiasi altro strumento ritenuto idoneo ad una più ampia diffusione dell'informativa.

Ogni utente che operi nell'ambito dell'Università, di norma, è tenuto a:

- ❑ utilizzare correttamente le apparecchiature date in uso o a cui accede via rete;
- ❑ adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche. In particolare, è tenuto alla conservazione dei codici di login e dell'indirizzo di rete assegnatigli ed a quanto stabilito nel presente Regolamento sull'accesso e uso delle risorse informatiche ad esso attribuite e dei servizi da esso fruiti;
- ❑ uniformarsi alle prescrizioni del presente Regolamento e segnalare eventuali violazioni alle medesime al Responsabile e agli Addetti della sicurezza informatica.

È vietata qualsiasi attività che possa produrre danni alle risorse informatiche dell'Università o che violi diritti di altri utenti e di terzi o che risulti in contrasto con le regole contenute nel presente Regolamento o con la normativa vigente o con le norme del GARR. In particolare, per quest'ultime sono attività proibite quelle riferite a:

- ❑ trasgressione della privacy di altri utenti o dell'integrità di dati personali;
- ❑ compromissione dell'integrità dei sistemi o dei servizi;
- ❑ consumo di risorse in misura tale da compromettere l'efficienza di altri servizi di rete;
- ❑ compimento di attività vietate dalla vigente normativa;

- ❑ accessi non autorizzati a risorse di rete e servizi o atti comunque inquadrabili tra la pirateria informatica.

### 5.1 Accesso ed uso delle aree e dei locali

Fulcro della base minima di sicurezza, da implementare in base alla normativa vigente, è il controllo fisico e logico degli accessi alle aree ed ai locali che consiste nel garantire che agli oggetti e gli apparati del sistema di comunicazione informatica si acceda esclusivamente secondo modalità prestabilite ed in base alle esigenze di sicurezza presenti ed alle funzionalità cui è adibito il singolo locale.

In genere, il controllo fisico va dal normale servizio di guardia e/o video-sorveglianza più o meno sofisticato, a sistemi di controllo della temperatura, antieffrazione, antintrusione, antisfondamento e di blindatura ed apertura tramite badge; mentre il controllo logico consiste in un adeguato sistema di autorizzazione ed autenticazione a partire dal prelievo/possesso di chiavi fino all'attribuzione di codici di login o smart card strettamente personali che permettono l'accesso solo a chi è formalmente autorizzato in base al proprio ruolo ed alle funzioni assegnate.

Per gli scopi del presente regolamento, sono coinvolti i seguenti luoghi di accesso:

- ❑ uffici, luoghi ed aree adibite a posti di lavoro riservati al personale dell'Ateneo ed eventualmente a collaboratori temporanei;
- ❑ laboratori, luoghi dedicati all'attività scientifica e di ricerca;
- ❑ locali tecnici, luoghi contenenti apparati e materiali informatici, telematici, di fonia e per la rete;
- ❑ aree informatizzate ossia aula informatica e/o polifunzionale, laboratorio e angolo/zona informatizzata, luoghi dove siano installati terminali di accesso ai servizi di rete.

Il controllo degli accessi riguarda, quindi, tutte le locazioni che contengono apparati e materiali di rete, impianti elettrici e di condizionamento, apparati di fonia e linee dati, supporti di backup, documenti e qualsiasi altro elemento richiesto per la gestione e manutenzione dei sistemi informatici e telematici, oltre che la protezione dei locali contenenti sistemi hardware. Esso restringe i diritti di accesso dei soggetti alle zone che ospitano risorse informatiche e non, accessi disciplinati da una procedura di carattere generale e da procedure specifiche per ogni singola zona.

Ciascun dipendente deve essere informato sulle aree di competenza in termini d'accesso fisico e logico e d'orario dell'accesso consentito.

Per le procedure di carattere generale, riguardanti le aree non informatizzate, si rinvia alle vigenti norme in uso presso l'Ateneo, mentre per le aree informatizzate di cui al terzo comma del presente articolo si rinvia all'apposito Regolamento.

Per gli uffici ed i laboratori, non occorrono procedure specifiche, fermo restando le procedure vigenti di carattere generale ed applicando quanto stabilito all'art. 5.2 del presente Regolamento.

Per i locali tecnici, divisi o compartimentati secondo diversi livelli di abilitazioni di accesso dipendenti dalle esigenze di sicurezza degli apparati presenti e dalle funzionalità cui è adibito il singolo locale, le procedure specifiche minime riguardano:

- ❑ l'installazione di impianti di condizionamento adeguati e di allarme, a gestione centralizzata, comprendenti sonde di rilevazione della temperatura del singolo locale;
- ❑ l'erogazione di corrente stabilizzata dai quadri elettrici, mediante UPS intelligenti che permettono di programmare uno spegnimento soft degli apparati connessi;
- ❑ il riscontro di intrusioni fisiche tramite un sistema di monitoraggio, con eventuale controllo da remoto, degli allarmi provenienti da rilevatori volumetrici di presenze che premuniscono da eventuali effrazioni di porte e finestre;
- ❑ un sistema di autorizzazione/autenticazione informatica.

Gli accessi alle aree ed ai locali tecnici avvengono tramite l'uso di smart card, strettamente personali e rilasciati esclusivamente al personale conosciuto, che attivano l'apertura della porta di ingresso solo se il possessore della carta è compreso nel data base dei permessi per quel locale. Il personale deve essere preventivamente legittimato, su formale e preventiva autorizzazione, in base

al ruolo ed alle sue specifiche funzioni e mansioni in materia informatica ed in relazione all'uso e alle funzionalità cui è adibito il singolo locale.

Ne consegue che, per quanto attiene il centro stella principale dell'Ateneo, suddiviso in quattro locali separati ad accesso differenziato mediante smart card, in base alla compartimentazione effettuata, si avrà:

- il locale centro stella fonia a cui possono accedere i soggetti cui è affidata formalmente la sicurezza informatica, la gestione tecnica della fonia e, sotto supervisione di quest'ultimi, i gestori esterni del servizio ed altri soggetti per attività inerenti i servizi e gli apparati ivi presenti;
- il locale centro stella dati a cui possono accedere i soggetti cui è affidata formalmente la sicurezza informatica e la gestione della struttura di Rete dell'Ateneo e, sotto loro supervisione, altri soggetti per progetti ed attività inerenti la rete o le connessioni ed inerenti i servizi e gli apparati ivi presenti;
- il locale server farm d'Ateneo a cui possono accedere i soggetti cui è affidata formalmente la sicurezza informatica, la gestione dei server e dei servizi presenti e del sistema informativo di Ateneo e, sotto supervisione di quest'ultimi, altri soggetti per attività inerenti i servizi e gli apparati ivi presenti;
- il locale server farm di II livello, a cui possono accedere i soggetti cui è affidata formalmente la sicurezza informatica, la gestione e la sicurezza dei server presenti, del sistema informativo di Ateneo, dei data base e dei loro applicativi e, sotto loro supervisione, gli eventuali gestori esterni degli applicativi ed altri soggetti per attività inerenti i servizi e gli apparati ivi presenti.

In merito ai locali tecnici di piano, equiparabili in funzionalità al locale centro stella dati, ad essi potrà accedere il personale cui è affidata formalmente la sicurezza informatica e la gestione della struttura di rete e, sotto loro supervisione, altri soggetti per attività inerenti i servizi e gli apparati ivi presenti.

## **5.2 Accesso ed uso delle risorse informatiche**

Qualsiasi accesso alla rete, alle risorse ed ai servizi con essa offerti è permesso agli utenti che, per motivi di servizio o istituzionali, ne devono fare uso, mediante l'utilizzo di credenziali, in genere l'indirizzo di rete assegnato al personal computer e, ove occorra, il codice di login personale assegnato dal Centro di Calcolo Elettronico o dal Responsabile informatico e/o dei dati, ed associati ad una persona fisica cui imputare le attività svolte per loro tramite.

Le modalità di accesso ed uso delle risorse informatiche variano a seconda delle classi di utenti e di servizi e possono richiedere l'assegnazione di codici di login personali e non cedibili, così come descritto nel presente Regolamento.

In ogni caso, l'utente deve firmare e consegnare un modulo di assunzione di responsabilità, disponibile su Web, impegnandosi a rispettare la normativa vigente e le regole internazionali dell'RFC 1855 "Netiquette Guidelines" e ogni altra norma o regola emessa dall'Ateneo, dal GARR, da altre autorità nazionali ed internazionali ed eventualmente da altro Ente locale.

L'accesso è assicurato compatibilmente con le potenzialità delle attrezzature. In genere, l'autorizzazione all'accesso alla rete o ad uno specifico servizio si considera concessa, senza alcuna formalità aggiuntiva, se e solo se riguarda l'uso di risorse pubbliche (World Wide Web, FTP Anonimo, servizi bibliotecari dalle postazioni della Biblioteca centrale, aule informatiche, mostre e manifestazioni ufficiali e similari) e/o il richiedente è titolare del diritto di accesso in quanto utente dell'Ateneo.

Gli accessi esterni alle risorse informatiche dell'Ateneo avvengono mediante gli apparati di connessione alla Rete GARR e alla rete metropolitana gestiti dal Centro di Calcolo Elettronico. Altri tipologie, come accessi dall'esterno attraverso linea commutata, sono di norma rigorosamente vietati; tuttavia, in casi eccezionali e motivati da reali esigenze istituzionali, previo richiesta inoltrata al Centro di Calcolo Elettronico, l'autorizzazione potrà essere concessa se previsti con autenticazione di ingresso (login, password, controllo e riconoscimento del numero chiamante) e

con misure di sicurezza atte a prevenire intrusioni e/o utilizzi illeciti, nonché dietro firma e consegna del modulo di assunzione di responsabilità.

Alla fine del periodo di utilizzazione della rete, delle risorse e dei servizi con essa offerti, l'utente è tenuto a effettuare correttamente l'operazione di logout ovvero di uscita dalle risorse e dai servizi fruiti, nonché di spegnimento del personal computer, se al termine della propria attività lavorativa.

Il Centro di Calcolo Elettronico, cui è demandata la gestione delle risorse e dei servizi di rete dell'Ateneo, assegna a ciascun utente e/o struttura, secondo criteri organizzativi e tecnici individuati dal Centro stesso e pubblicati sul sito web d'Ateneo, previa richiesta scritta opportunamente autorizzata:

- ❑ un indirizzo di rete, fisico e logico;
- ❑ un codice di login personale per l'accesso alle risorse informatiche, ove gestite direttamente;
- ❑ un account di posta elettronica;
- ❑ uno spazio per la pubblicazione di pagine web statiche o dinamiche.

Per l'accesso alle risorse informatiche e ai dati non gestiti tramite il Centro di Calcolo Elettronico, il codice di login personale e non cedibile va richiesto al relativo Responsabile della struttura e/o informatico e/o dei dati che autorizza formalmente l'utente assegnandolo e dando indicazioni sull'uso corretto delle risorse informatiche cui si riferisce.

Ogni applicazione che abbia un impatto significativo sulla disponibilità della banda di un tratto di rete locale dell'Ateneo, metropolitana o geografica, deve essere preventivamente segnalata al Centro di Calcolo Elettronico, che in collaborazione con il Responsabile della struttura e/o informatico e/o dei dati, ne cura l'esecuzione verificando la compatibilità dell'applicazione con la fruizione degli altri servizi.

E' vietato l'accesso alle risorse, alla rete e/o ai servizi contemporaneamente da più personal computer usando lo stesso codice di login.

È vietato impedire o interferire o tentare di impedire o interferire in qualsiasi forma con i servizi offerti tramite la Rete d'Ateneo agli altri utenti e manomettere in qualsiasi modo le apparecchiature e le strutture informatiche ed elettroniche.

È vietato l'uso illecito e/o il tentativo di accesso fraudolento e/o l'accesso non autorizzato a qualsiasi risorsa di rete disponibile localmente o sulla rete esterna.

È altresì vietato distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare o accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili.

Il Responsabile e gli Addetti della sicurezza informatica ovvero il Responsabile informatico e/o dei dati sono autorizzati e possono, fatte salve le responsabilità amministrative e penali, disattivare in qualsiasi momento un codice di login e/o una password, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento dei sistemi ovvero qualora vi sia fondato sospetto che l'utente abbia violato il presente Regolamento.

### **5.3 Accesso ed uso della Rete d'Ateneo**

La Rete d'Ateneo può essere utilizzata esclusivamente per gli scopi autorizzati dal presente Regolamento, vale a dire come supporto alla ricerca, alla didattica, all'amministrazione, e alle altre attività di servizio ed istituzionali dell'Università, nonché per l'accesso a siti di pubblico interesse e come strumento utile alla comunità dell'Ateneo.

In genere, la connessione, anche temporanea, di un client o di un server alla Rete di Ateneo avviene dietro autorizzazione del Responsabile della struttura di appartenenza e dopo aver richiesto ed ottenuto un indirizzo di rete, numerico e logico, e la relativa configurazione dal Centro di Calcolo Elettronico direttamente o per tramite del Responsabile e/o Referente informatico. È consentita la

sostituzione dei dispositivi (elaboratore, periferica, etc.) connessi alla rete purché non influenzino la sua funzionalità.

L'autoassegnazione dell'indirizzo di rete è espressamente vietata e l'utente otterrà l'autorizzazione all'accesso alla Rete d'Ateneo, anche se solo temporaneamente, se e soltanto se identificato ed identificabile.

A tale scopo, l'utente acconsentirà al trattamento dei suoi dati personali da parte dell'Ateneo, in conformità alle norme legislative e regolamentari vigenti e applicabili, sottoscrivendo l'apposito modulo di assunzione di responsabilità predisposto dal Centro di Calcolo Elettronico che sarà reso disponibile anche sul sito web d'Ateneo.

Egli otterrà l'autorizzazione dopo essersi impegnato ad osservare il presente Regolamento e rispettare le regole internazionali dell'RFC 1855 "Netiquette Guidelines" e ogni altra norma o regola emessa dall'Ateneo, dal GARR, da altre autorità nazionali ed internazionali disciplinanti le attività e i servizi che si svolgono per il tramite della Rete d'Ateneo.

L'indirizzo di rete assegnato è personale e non cedibile e l'utente assegnatario è totalmente responsabile delle attività svolte per suo tramite e, pertanto, egli è tenuto a comunicarne al Centro di Calcolo Elettronico, direttamente o per tramite del Responsabile e/o Referente informatico, l'eventuale dismissione.

Per i sistemi collegati in rete su cui possono operare più utenti deve essere nominato un responsabile al quale verrà assegnato l'indirizzo di rete; tale responsabile dovrà garantire la conservazione dei dati necessari all'identificazione dei vari utenti utilizzatori in ogni istante di collegamento alla Rete d'Ateneo.

La procedura di autorizzazione, di cui ai commi precedenti, può non essere richiesta nel caso di utilizzo di risorse pubbliche o comunque dedicate a larghe categorie di utenti, interni ed esterni, come l'accesso ai servizi web o a quelli bibliotecari dalle postazioni della Biblioteca centrale d'Ateneo, dove essa si considera concessa a chiunque abbia diritto al servizio, limitatamente alle risorse necessarie per usufruire del diritto stesso e senza alcuna formalità aggiuntiva, ovvero per eventi particolari, quali mostre o manifestazioni o similari, deliberati da Organi dell'Ateneo per i quali può esserne autorizzato l'uso a terzi, anche al pubblico, limitato nel tempo e nelle risorse, senza alcuna formalità aggiuntiva, sempre che preventivamente si sia avuta la necessaria ammissibilità dal Responsabile amministrativo dei domini e delle reti.

Nessuna struttura può autorizzare alcun accesso alla Rete d'Ateneo a persone o ad Enti al di fuori dei casi sopra riportati.

È vietato utilizzare la Rete per scopi incompatibili con quelli stabiliti nel presente Regolamento. In particolare, a titolo esemplificativo e non esaustivo, è vietato:

- ❑ accedere alla Rete d'Ateneo per conseguire l'accesso non autorizzato a qualsiasi risorse di rete interne od esterne all'Università;
- ❑ fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso alla Rete d'Ateneo. Nel caso ne venga a conoscenza il Responsabile della struttura e/o informatico di appartenenza dell'indebito fornitore di accesso, ha l'obbligo di disporre la cessazione dell'abuso o illecito, dopo averne comunicato lo stato alla persona indebitamente beneficiaria; in difetto dell'azione da parte dei summenzionati Responsabili, il Responsabile e gli Addetti della sicurezza informatica ovvero il personale preposto del Centro di Calcolo Elettronico mettono in atto tutti gli accorgimenti tecnici disponibili per disattivare ogni trasporto relativo ad applicazioni della persona indebitamente beneficiaria;
- ❑ usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi. Il Responsabile e gli Addetti della sicurezza informatica, nonché il personale preposto del Centro di Calcolo Elettronico hanno la facoltà di impedire in qualsiasi momento l'accesso alla Rete d'Ateneo da parte di utenti anonimi o non sufficientemente identificati o identificabili;
- ❑ violare gli obblighi contrattualmente assunti dall'Università per la realizzazione e la gestione della Rete d'Ateneo, particolarmente in materia di copyright, licenze d'uso di software e regolamenti dei fornitori di connettività di rete;

- ❑ svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, distruggano risorse, danneggino o restringano l'utilizzabilità o le prestazioni della Rete d'Ateneo;
- ❑ violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni, intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete d'Ateneo, dei quali non si è destinatari specifici;
- ❑ compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
- ❑ creare o diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno. In particolare, è vietato la ricezione, la trasmissione o il possesso d'immagini pornografiche relative a minori;
- ❑ utilizzare la Rete d'Ateneo e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale, tranne nei casi specificatamente autorizzati dal Rettore.

Il Responsabile e gli Addetti della sicurezza informatica ovvero il Responsabile informatico sono autorizzati, fatte salve le responsabilità amministrative e penali, a disattivare in qualsiasi momento un indirizzo di rete, disconnettere un sistema in rete, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento della Rete d'Ateneo, nel caso di uso illecito di qualsiasi risorsa di rete disponibile ovvero qualora vi sia fondato sospetto che l'utente utilizzatore abbia violato il presente Regolamento.

#### **5.4 Accesso ed uso del software**

Qualsiasi software, sia esso inerente alla didattica, alla ricerca o all'attività amministrativa, a qualsiasi titolo acquisito o dato in uso o realizzato dall'Università, deve essere protetto da distruzioni o perdite anche accidentali, alterazioni, usi illeciti e divulgazioni non autorizzate e non può essere utilizzato per scopi commerciali.

Qualsiasi software non espressamente rilasciato con strumenti finalizzati alla diffusione pubblica (WWW, FTP e similari) è da intendersi riservato e la sua copia e/o utilizzo, fermo restando le norme sul copyright e i diritti d'autore, devono essere espressamente autorizzati dal Responsabile della struttura a cui esso è assegnato.

La distribuzione gratuita di software da parte può avvenire purché, utilizzando di volta in volta gli strumenti più idonei e le formulazioni più appropriate, vengano informati i potenziali utilizzatori delle seguenti condizioni:

- ❑ l'Università non fornisce alcuna garanzia sui software distribuiti gratuitamente e, in particolare, non garantisce la loro adeguatezza e fruibilità per scopi specifici;
- ❑ in nessun caso l'Università potrà essere ritenuta responsabile per danni diretti, indiretti o derivanti dall'uso dei software distribuiti gratuitamente o dai risultati da essi forniti. In particolare non potrà essere ritenuta responsabile per eventuali ritardi, inadempienze, perdita di dati e danni economici derivanti o in qualche modo collegati all'uso di tali software od ai risultati da essi forniti.

#### **5.5 Accesso ed uso dei servizi**

Qualsiasi accesso ai servizi offerti con le risorse informatiche disponibili presso l'Ateneo, di norma, è permesso agli utenti che, per motivi di servizio o istituzionali, ne devono fare uso, sulla base di criteri organizzativi e tecnici che possono comprendere anche l'assegnazione di codici di login personali da parte del Centro di Calcolo Elettronico o del Responsabile informatico e/o dei dati cui fa capo il servizio, e che sono pubblicati anche sui siti web d'Ateneo.

Le modalità di accesso ed uso dei servizi variano a seconda delle classi di utenti e della loro tipologia pubblica o ristretta o riservata. In ogni caso, l'utente può accedere solo a quei servizi per i quali è stato espressamente autorizzato, nel rispetto della normativa vigente, delle regole nazionali ed internazionali e delle regole del presente Regolamento, e con le modalità consentite. Egli è

personalmente e formalmente responsabile del mantenimento della necessaria riservatezza sui propri codici di login e sulle password ad essi associate, nonché delle attività svolte per loro tramite.

L'utente si impegna a comunicare immediatamente al Responsabile e/o Referente informatico della propria struttura lo smarrimento, il furto o l'appropriazione da parte di terzi dei propri codici di login e/o delle proprie password; questi deve riferirne tempestivamente al personale preposto del Centro di Calcolo Elettronico ovvero al Responsabile informatico della struttura offerente il servizio.

L'utente è tenuto a segnalare immediatamente qualsiasi errore o malfunzionamento dei servizi di cui sia venuto a conoscenza al Responsabile e/o al Referente informatico della propria struttura, il quale, dopo aver appurato che non si tratti di problemi di sua competenza, deve riferirne tempestivamente al personale preposto del Centro di Calcolo Elettronico ovvero al Responsabile informatico della struttura offerente il servizio.

### ***DNS (Domain Name System)***

Ogni sistema/servizio di rete deve avere un unico indirizzo numerico di rete ed un corrispondente nome logico di dominio registrato nel DNS d'Ateneo.

L'indirizzo di rete viene assegnato dal personale preposto del Centro di Calcolo Elettronico su richiesta dell'utente ovvero del Responsabile e/o del Referente informatico della struttura di appartenenza con cui viene concordato il corrispondente logico.

È compito del Responsabile e/o del Referente informatico mantenere aggiornata la lista degli indirizzi di rete assegnati alla propria struttura, comunicando tempestivamente al Centro di Calcolo Elettronico ogni loro variazione.

Anche per quanto riguarda l'utilizzo di alias all'interno del dominio di struttura è il Responsabile e/o il Referente informatico che deve richiederne l'attivazione ovvero comunicarne la variazione al Centro di Calcolo Elettronico.

### ***Posta elettronica***

L'indirizzo di posta elettronica sotto il dominio "uniparthenope.it" viene concesso unicamente a tutti i suoi utenti ed a tutte le sue strutture e ad esso corrisponde una casella di posta elettronica sui server ufficiali dell'Ateneo strettamente personale e l'utente, cui essa è associata, si assume ogni responsabilità per un suo utilizzo improprio come l'invio di messaggi con contenuto offensivo, diffamatorio, osceno, indecente o che attentino alla dignità umana e/o di informazioni o pubblicità non richieste (spam) e non autorizzati.

Di norma, l'utente presenta un'apposita richiesta dove acconsente al trattamento dei propri dati personali da parte dell'Ateneo, in conformità alle norme legislative e regolamentari vigenti ed applicabili, e sottoscrive l'apposito modulo di assunzione di responsabilità predisposto dal Centro di Calcolo Elettronico che sarà reso disponibile anche sul sito web d'Ateneo. Egli, in tal modo, si impegna ad osservare il presente Regolamento ed a rispettare le regole internazionali dell'RFC 1855 "Netiquette Guidelines" e ogni altra norma o regola emessa dall'Ateneo, dal GARR, da altre autorità nazionali ed internazionali, disciplinanti le attività e i servizi che si svolgono per il tramite della Rete d'Ateneo.

È possibile accedere alla propria casella di posta elettronica secondo due modalità: localmente tramite un qualsiasi client di posta elettronica, opportunamente configurato, o da remoto per mezzo di un browser web.

Al momento dell'attivazione, la casella di posta elettronica viene creata con una configurazione standard: alcuni parametri, quale ad esempio l'indirizzo logico associato, non sono modificabili direttamente dall'utente, che comunque può chiederne la modifica al postmaster del Centro di Calcolo Elettronico. L'utente può, invece, personalizzare la propria casella modificando alcuni parametri, quali ad esempio l'attivazione/disattivazione di messaggi di risposta automatica.

Ogni utente è reperibile con indirizzi di posta del tipo "nome.cognome@uniparthenope.it", caselle di posta strettamente personali e con password di accesso anch'esse personali e non cedibili.

Ciascuna Struttura viene dotata d'ufficio di un indirizzo di posta elettronica del tipo "nomestruttura@uniparthenope.it"; in tal caso il Responsabile della struttura deve nominarne un responsabile per il quale valgono le stesse regole di cui al comma precedente.

Possono essere settati indirizzi del tipo "servizio" ovvero "sigla" e "@uniparthenope.it" per le caselle che fanno riferimento ad un servizio o ad esigenze particolari e gli utenti possono avere indirizzi diversi da quello ufficiale attraverso meccanismi di tipo forwarding o aliases implementati sui server ufficiali di Ateneo.

### **Fonia**

Le modalità di fruizione del servizio variano, a seconda della tipologia della richiesta (nuove linee, spostamento/variazione delle esistenti e guasti), sulla base di criteri organizzativi e tecnici individuati dal personale preposto del Centro di Calcolo Elettronico e pubblicati anche sul sito web d'Ateneo.

In genere, se in una qualsiasi struttura dell'Ateneo sorge la necessità di avere una nuova linea telefonica interna o di variare una qualsiasi specifica o requisito di una linea interna esistente oppure di spostare una linea interna esistente presso altri locali e/o altra sede, il Responsabile della struttura deve far pervenire una richiesta al personale preposto del Centro di Calcolo Elettronico. Ricevuta la richiesta, il summenzionato personale provvederà a girarla al fornitore esterno e, se necessario, a sollecitare l'intervento richiesto.

È cura del Responsabile della Struttura riconoscere il singolo numero telefonico assegnato, autorizzandone l'attivazione da parte del personale preposto, come appartenente al proprio centro di costo; inoltre, egli ne decide le abilitazioni e ne assicura la correttezza dell'utilizzo qualora accessibile da parte di più persone fisiche.

È cura del singolo utente assegnatario comunicare ogni variazione della propria situazione al personale preposto del Centro di Calcolo Elettronico, verificandone inoltre la correttezza nella rubrica on-line di Ateneo.

È vietata l'attivazione di singole linee o di sistemi di fonia esterni al sistema di fonia di Ateneo, fatta salva un'espressa autorizzazione, per eccezionali e comprovate esigenze, da parte degli organi competenti. Ogni attivazione di singole linee o di sistemi di fonia esterne deve essere tempestivamente comunicata al personale preposto del Centro di Calcolo Elettronico ed agli Organi Contabili dell'Ateneo.

È espressamente vietato il collegamento di apparecchiature attive o passive non rispondenti alle caratteristiche tecniche richieste dalla specifica attivazione della singola "presa utente", potendo comportare anche danneggiamenti al sistema di fonia di Ateneo ed agli stessi dispositivi collegati.

### **5.6 Accesso e uso ai dati e alle informazioni**

Qualsiasi dato non espressamente rilasciato con strumenti finalizzati alla diffusione pubblica di informazioni, come il web o i depositi FTP, è da intendersi riservato ed il suo accesso ed uso deve essere espressamente autorizzato dal relativo Responsabile.

Fermo restando quanto stabilito dal D.Lgs. n. 196/2003, l'accesso ai dati personali internamente all'Ateneo non è consentito, se non per il perseguimento dei fini istituzionali dell'Università e per il tramite dei responsabili e degli incaricati, su formale e motivata richiesta da parte degli organi, delle strutture, e del personale dell'Ateneo. Tale richiesta dovrà essere connessa con lo svolgimento dell'attività inerente alla specifica funzione del richiedente e verrà soddisfatta in via diretta ed esclusivamente nella misura necessaria al perseguimento dell'interesse istituzionale.

Le richieste avanzate da enti o da terzi, necessarie al perseguimento dei fini istituzionali del richiedente, secondo quanto da questi dichiarato, e finalizzate ad ottenere il trattamento, la comunicazione o la diffusione di dati personali, non possono essere soddisfatte ove non abbiano forma scritta e siano prive di motivazione. Esse dovranno essere accompagnate da una dichiarazione con la quale il richiedente si impegna ad utilizzare i dati esclusivamente per lo scopo e con le modalità indicate nella richiesta ed indicare il nome, la denominazione, o la ragione sociale

del richiedente, i dati cui la domanda si riferisce, lo scopo della richiesta e le modalità di utilizzazione dei dati e l'eventuale ambito di comunicazione e diffusione dei dati.

La comunicazione e la diffusione di dati da parte dell'Ateneo sono comunque consentite quando:

- ❑ siano previste da norme legislative o regolamentari, statali o regionali, o da regolamenti comunitari;
- ❑ siano necessarie per scopi di ricerca scientifica o statistica, sempre che si tratti di dati anonimi e/o aggregati;
- ❑ siano richieste dai soggetti di cui all'art. 4, comma 1, lettere (b), (d), (e), della legge, per scopi di difesa o di sicurezza dello Stato, di prevenzione, accertamento o repressione di reati;
- ❑ siano necessarie a soddisfare richieste di accesso ai documenti amministrativi ai sensi dell'art. 22 della legge 7 agosto 1990, n. 241.

Sono altresì consentite, senza la necessità del consenso dell'interessato, la diffusione e la comunicazione a terzi di dati relativi, al personale, anche cessato, docente, ricercatore, e tecnico-amministrativo dell'Ateneo, ai collaboratori professionali anche esterni, aventi a qualsiasi titolo un rapporto di lavoro con l'Ateneo, nonché ai soggetti estranei all'Amministrazione che siano membri di organi collegiali o commissioni dell'Ateneo, limitatamente ai dati seguenti:

- ❑ il nome, la qualifica, e i dati a questa inerenti, ad esclusione del trattamento economico individuale;
- ❑ la sede di servizio, nonché il numero telefonico, il numero di fax, e l'indirizzo di posta elettronica;
- ❑ la struttura di appartenenza e l'organo collegiale di cui l'interessato sia membro.

Il responsabile del trattamento, accertato che il trattamento, la comunicazione, o la diffusione non siano incompatibili con i fini istituzionali dell'Università, trasmette i dati nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.

L'Ateneo consente la comunicazione e diffusione di dati riguardanti studenti e diplomati, su richiesta di soggetti pubblici e privati, al fine di favorirne le esperienze professionali e la collocazione nel mondo del lavoro.

### **5.7 Accesso ed uso di risorse informatiche esterne all'Ateneo**

L'accesso e l'uso di risorse informatiche esterne all'Università e da essa non dipendenti è soggetto, nel rispetto del vigente ordinamento, alle norme ed ai regolamenti fissati dei titolari di tali risorse, oltre che all'RFC 1855 "Netiquette Guidelines", alle norme GARR ed ogni altra legge o regolamento relativo alla particolare rete utilizzata e agli standard IETF.

Ogni soggetto che utilizzi risorse informatiche esterne all'Ateneo è tenuto ad adottare tutte le misure necessarie per non interferire nel corretto funzionamento delle comunicazioni e per evitare che le attività svolte producano danni ai titolari delle risorse utilizzate.

### **6.0 Gestione della sicurezza e degli incidenti**

Da considerazioni in merito alle vulnerabilità dei sistemi e dei servizi di rete dell'Ateneo, alle minacce e ai danni cui sono sottoposti, alle tipologie di traffico veicolato dalla Rete d'Ateneo, si ritiene che le direttive di sicurezza devono essere coerenti con una situazione di medio rischio informatico. In particolare, le considerazioni effettuate sono:

- ❑ la vulnerabilità dei servizi di rete è elevata, sia per i protocolli utilizzati (IPv4) sia per la situazione non omogenea delle varie strutture d'Ateneo che erogano servizi di rete non armonizzati tra loro;
- ❑ le minacce sono diverse, ma riconducibili alle tipologie di accessi non autorizzati, sia dall'esterno sia dall'interno. Sono molto frequenti e spesso non hanno obiettivi distruttivi, ma rappresentano semplicemente una "sfida". In particolare, le modalità di intrusione possono essere:
  - minacce alla proprietà/riservatezza/autenticità/integrità/disponibilità dell'informazione;

- cattura di passwords;
  - acquisizione dei privilegi di amministratore di sistema da parte di soggetti non autorizzati;
  - mail spamming;
  - diffusione di virus informatici;
  - denial-of-service.
- i danni possono essere dovuti all'interruzione o al malfunzionamento dei servizi, con conseguente penalizzazione dell'attività e dell'immagine dell'Ateneo verso l'esterno, ed all'uso dei servizi di rete dell'Ateneo per commettere crimini informatici, anche verso terzi, con eventuale conseguente azione giudiziaria nei confronti dell'Ateneo;
  - i dati critici ossia quelli personali, sensibili e amministrativi veicolati dalla rete d'Ateneo rappresentano, al momento, una percentuale bassa rispetto al dato complessivo;
  - la posta elettronica ed i servizi web sono strumenti destinati a svolgere un ruolo primario in tutte le attività dell'Ateneo e come tali devono essere armonizzati ed affidabili.

Da queste considerazioni si può facilmente concludere che l'alta vulnerabilità dei servizi è compensata dalla bassa criticità dei dati, con un conseguente rischio risultante di livello medio.

Tutti i sistemi in rete, in base alle normative vigenti, devono essere mantenuti costantemente in adeguate condizioni di sicurezza ed il Responsabile della sicurezza informatica d'Ateneo deve garantire il rispetto di tutte le leggi e i regolamenti vigenti, in particolare quelle che riguardano la sicurezza e gli incidenti informatici.

A tale scopo le Strutture che intendono offrire servizi di rete sono tenute a segnalarli preventivamente al Responsabile della sicurezza informatica, il quale verifica che siano garantite le condizioni minime di sicurezza per l'avvio del servizio. In particolare, dovranno essere assicurati:

- la presenza di un Responsabile informatico, con funzioni di gestore del servizio che garantisca la continuità del servizio stesso e che collabori con il personale preposto del Centro di Calcolo Elettronico per la sua armonizzazione con i restanti servizi;
- l'aggiornamento costante del servizio in modo che non sia affetto da vulnerabilità note che ne potrebbero compromettere la sicurezza informatica;
- monitoraggio e conservazione per il periodo previsto dalla normativa vigente della registrazione degli accessi al servizio in file di log, in modo da consentire al Responsabile e agli Addetti della sicurezza informatica eventuali indagini interne o richieste dalle Autorità esterne in caso di uso improprio delle risorse;
- l'assicurazione verso l'utenza che dette registrazioni non sono disponibili ad alcuno se non nei casi di emergenza, riconosciuti come tali dal Responsabile della sicurezza informatica, nel rispetto della normativa vigente.

La notifica di un servizio di rete da attivare presso una struttura va inoltrata al Responsabile della sicurezza informatica, secondo le norme da esso definite, sottoscritta dal Responsabile della struttura e contenente obbligatoriamente la descrizione del servizio e le caratteristiche tecniche del server che fornirà il servizio (sistema operativo, nome, indirizzo di rete, nome e versione dell'applicazione e quanto sia ritenuto utile), se non appartenente a quelli disponibili presso il Centro di Calcolo Elettronico. Valutata la richiesta, il Responsabile della sicurezza informatica risponderà comunicando le misure di sicurezza da adottare per il particolare servizio.

Il Responsabile informatico della Struttura che ospita il servizio, è tenuto a segnalare al Responsabile della sicurezza informatica immediatamente intrusioni o tentativi di intrusione che abbiano avuto come oggetto l'elaboratore che eroga il servizio, mettendo a disposizione i dati delle registrazioni sopradescritte.

Nel caso in cui, a seguito di controlli, segnalazioni o incidenti, il Responsabile della sicurezza informatica rilevi l'inadeguatezza di sistema/servizio per quanto riguarda la sicurezza diretta o indiretta, detto sistema/servizio dovrà essere immediatamente adeguato, secondo le indicazioni da lui fornite, o staccato dalla rete a cura della Struttura di appartenenza.

In difetto dell'azione da parte della Struttura o nel caso in cui il servizio non sia stato autorizzato, saranno messi in atto tutti gli accorgimenti tecnici disponibili per disattivare ogni

trasporto sulla rete relativo al sistema/servizio inadeguato, sino all'intervento correttivo operato dalla Struttura.

È compito dei responsabili della rete e dei sistemi predisporre meccanismi tecnici ed organizzativi per il loro monitoraggio periodico, anche quotidiano.

In caso di rilevazione di incidente, il Responsabile della struttura coinvolta ed il Responsabile della sicurezza informatica devono essere tempestivamente avvisati. Essi informeranno, a loro volta, gli Organi Accademici e le strutture che possono essere potenzialmente coinvolte, e predisporranno le necessarie contromisure.

I responsabili dei sistemi devono provvedere nel più breve tempo possibile al ripristino del servizio, a meno che, di comune accordo con il Responsabile della struttura ed il Responsabile della sicurezza informatica, non venga deciso di individuare prioritariamente la causa dell'incidente interrompendo temporaneamente il servizio stesso. Essi, comunque, dovranno salvare i file modificati prima del loro ripristino e mantenere adeguatamente le informazioni utili per la descrizione dell'incidente.

Sarà cura del Comitato per la sicurezza informatica, di concerto con i Responsabili delle strutture offerenti servizi ed il Responsabile e gli Addetti alla sicurezza informatica, redigere un piano particolareggiato di ripristino per i sistemi, i servizi ed i dati. In tale piano dovrà essere stabilito, sulla base delle responsabilità e degli incarichi formalmente riconosciuti, le misure per la sicurezza della conservazione delle password privilegiate; chi può essere formalmente autorizzato al loro uso ed in che modo, in caso di irreperibilità del responsabile; le modalità e la periodicità delle operazioni di backup del sistema e dei dati; la prassi da seguire per il ripristino del sistema e dei servizi.

## **7.0 Responsabilità**

L'Ateneo stabilisce di adottare norme che, coerentemente con le finalità istituzionali dell'Università e compatibilmente con il contesto normativo e tecnico di riferimento, basandosi sui principi di massima circolazione interna delle informazioni e di ampia visibilità esterna di informazioni relative alla propria attività istituzionale, si pongono l'obiettivo di garantire il più possibile l'utilizzo efficiente delle risorse e dei servizi di rete, anche grazie al decentramento dell'assunzione di responsabilità.

L'Università, in qualità di fornitore dei documenti accessibili attraverso la Rete d'Ateneo, è responsabile unicamente dei contenuti dei documenti da essa messi direttamente a disposizione. Essa non è responsabile dei contenuti di altri siti o pagine Internet ai quali sia fatto collegamento mediante link.

### **7.1 Responsabilità individuali**

I soggetti che utilizzano risorse informatiche devono rispettare le regole fissate dal presente Regolamento ed in particolare:

- ❑ utilizzare le risorse informatiche per i soli scopi istituzionali ed in modo da non inficiare la loro regolare operatività e fruibilità da parte di altri utenti;
- ❑ mantenere una adeguata riservatezza dei dati, propri, di altri utenti e di terzi;
- ❑ mantenere una adeguata riservatezza sulle misure di sicurezza adottate e sulle modalità di accesso ai servizi;
- ❑ utilizzare esclusivamente le risorse alla cui fruizione essi sono abilitati e con le modalità stabilite dal presente Regolamento;
- ❑ osservare comportamenti di condotta personale, in conformità a principi di autodisciplina, tali da rispettare la normativa vigente, non provocare danni, sovraccaricare i sistemi e/o la rete, monitorare o controllare risorse informatiche senza averne esplicita autorizzazione, distrarre risorse;
- ❑ segnalare ogni accertata violazione delle norme che regolano l'utilizzo delle risorse informatiche al Responsabile informatico della struttura di appartenenza.

## 7.2 Responsabili delle strutture

I Responsabili delle Strutture sono i Direttori delle strutture operanti in ambito universitario, indipendentemente dalla funzione organizzativa a cui presiedono ed alla struttura a cui appartengono (Dipartimento, Centro, Presidenza, Laboratorio, Biblioteca e così via).

Essi dovranno adottare misure idonee per un corretto utilizzo delle risorse informatiche disponibili presso la loro struttura, esercitando una funzione di indirizzo e controllo, affinché:

- chiunque afferisca alla struttura operi secondo le regole contenute nel presente Regolamento,
- siano individuate ed assegnate con precisione le responsabilità per la gestione dei dati, per la gestione delle risorse informatiche e per la concessione eventuale di codici di login personali per l'accesso alle banche dati gestite localmente.

Essi possono delegare le funzioni operative a collaboratori di comprovata competenza tecnica, di cui agli articoli successivi, e predispongono tutte le condizioni organizzative, logistiche ed amministrative affinché questi possano svolgere efficacemente il proprio mandato, ivi compresa la loro formazione permanente.

Possono, inoltre, emanare regolamenti di accesso alle risorse con validità interna alla struttura, purché conformi con il presente Regolamento.

## 7.3 Responsabili dei dati

I Responsabili dei dati devono curare che, negli ambiti di loro competenza, le informazioni utilizzate per le attività istituzionali siano raccolte in modo accurato e mantenute aggiornate e disponibili per tutti gli usi consentiti.

Ai Responsabili dei dati è demandato il compito di autorizzare l'accesso alle informazioni riservate di propria competenza.

Le loro nomine, accolte dagli organi competenti mediante l'emanazione del relativo decreto, vanno formalmente comunicate al Centro di Calcolo Elettronico ed al Comitato per la sicurezza informatica.

## 7.4 Responsabili informatici

I Responsabili informatici sono nominati a tempo indeterminato dal Responsabile della struttura di appartenenza delle risorse; possono coincidere con i Responsabili dei dati e/o con i Referenti informatici. Essi, negli ambiti di loro competenza, sono responsabili dal punto di vista amministrativo e tecnico dei sistemi e dei servizi della struttura con obbligo di riferirsi al Responsabile della sicurezza informatica per ogni violazione o sospetto di violazione di sicurezza informatica e/o al presente Regolamento.

Essi devono provvedere a che le risorse informatiche siano mantenute efficienti e disponibili per tutti gli usi consentiti, collaborando con il personale preposto del Centro di Calcolo Elettronico e con il Responsabile e gli Addetti della sicurezza informatica per ridurre al minimo i rischi di incidente informatico. Devono, inoltre, operare secondo le direttive e le procedure prestabilite per la sicurezza dei sistemi e l'armonizzazione dei servizi, nel rispetto delle norme del presente Regolamento, adottando tempestivamente i provvedimenti previsti.

I Responsabili informatici provvedono a rendere operative le autorizzazioni all'accesso alle informazioni stabilite dai Responsabili dei dati e comunicano al Responsabile della sicurezza informatica ogni evento di rischio informatico.

Le loro nomine, rinunce o sostituzioni, accolte dagli organi competenti mediante l'emanazione del relativo decreto, vanno formalmente comunicate al Centro di Calcolo Elettronico ed al Comitato per la sicurezza informatica.

## 7.5 Referenti informatici

I Referenti informatici di struttura rappresentano l'interfaccia amministrativa e tecnica dell'utenza verso il Centro di Calcolo Elettronico, il Comitato per la sicurezza informatica ed il Responsabile della sicurezza informatica.

Essi curano la diffusione, all'interno dell'utenza gestita, delle notizie informatiche, procedurali ed organizzative comunicate, informando ed aggiornando inoltre tale utenza sulle proprie funzioni. Curano, inoltre, la distribuzione, nel rispetto delle norme amministrative e tecniche stabilite caso per caso, dei software licenziati centralmente.

Hanno l'obbligo di mantenere ed aggiornare l'associazione utente/indirizzo di rete e utente/interno telefonico, nonché di conoscere l'organizzazione fisica, logica e l'indirizzamento assegnati alla struttura di appartenenza.

## 8.0 Infrazioni

Nell'utilizzo delle risorse informatiche dell'Ateneo e nell'accesso alla rete ed ai servizi con essa offerti, non sono ammesse attività di tipo ricreativo e sono altresì vietate attività che possano produrre danni e disservizi alle risorse informatiche dell'Università o comunque illecite.

Costituisce infrazione:

- ❑ qualsiasi atto che possa compromettere la sicurezza e la riservatezza delle risorse informatiche dell'Università o di altri Enti fruibili attraverso le sue risorse informatiche;
- ❑ l'accesso, l'utilizzazione, la distruzione, l'alterazione o la disabilitazione non autorizzata di risorse informatiche, anche per mezzo di codici di login personali resi disponibili ad altri soggetti, nonché l'abbandono senza custodia di stazioni di lavoro già connesse a risorse informatiche riservate;
- ❑ l'uso di dati o di altre risorse informatiche per scopi non consentiti dalle norme vigenti;
- ❑ la duplicazione, l'archiviazione e l'uso di software su qualsiasi risorsa informatica dell'Università in violazione a disposizioni contrattuali;
- ❑ la violazione della riservatezza di altri utenti o terzi;
- ❑ l'uso dell'anonimato o il servirsi di risorse che consentano di restare anonimi;
- ❑ l'utilizzazione per scopi di interesse esclusivamente privato di qualsiasi risorsa informatica dell'Università;
- ❑ ogni tentativo di accesso fraudolento a dati e programmi altrui e ogni tentativo di utilizzo di codici di accesso diversi da quello di cui si è assegnatari;
- ❑ qualsiasi attività in contrasto con il presente Regolamento e con le vigenti norme civili, penali ed amministrative che disciplinano le attività e i servizi svolti sulla rete.

Tali infrazioni dovranno essere segnalate al Responsabile della sicurezza informatica che ne riferirà al Comitato per la sicurezza informatica e agli Organi Accademici competenti, al fine di adottare ogni misura necessaria per prevenire, reprimere e punire violazioni al presente Regolamento.

## 9.0 Sanzioni

La contravvenzione alle regole contenute nel presente Regolamento comporta la revoca delle autorizzazioni ad accedere alle risorse informatiche gestite dall'Università, fatte salve le più gravi sanzioni previste dalle norme vigenti.

I competenti Organi Accademici possono ordinare l'immediata cessazione dell'attività all'origine dell'abuso, adottando le necessarie misure per impedire ulteriori conseguenze ed individuare il responsabile. Accertata la violazione, sentito l'utente cui essa è imputata, con decisione motivata e fatte salve le ulteriori conseguenze di natura penale, civile, amministrativa e disciplinare della violazione compiuta, viene stabilita la sanzione che, in dipendenza della gravità della violazione stessa, va dall'esclusione, temporanea o permanente, dall'accesso alla Rete d'Ateneo e/o al servizio fino a sanzioni disciplinari eventualmente previste dallo statuto o dal contratto di lavoro.

La revoca delle autorizzazioni è assunta, avuta notizia dell'infrazione e valutata la gravità dell'illecito e delle eventuali conseguenze dannose prodotte o da prodursi, dalla Commissione per la Sicurezza Informatica dell'Ateneo e perdura sino all'intervento correttivo da parte del contravventore e/o della struttura di sua appartenenza.

Chi accede reiteratamente a qualsiasi risorsa della rete dell'Ateneo senza autorizzazione, dopo un primo invito ad astenersi dal farlo da parte di personale dell'Ateneo adibito al controllo o dal Responsabile della struttura competente o dal Responsabile o dagli Addetti della sicurezza informatica, perde il diritto a richiedere successivamente l'autorizzazione per un periodo di almeno un anno.

Chi, accedendo a risorse dell'Ateneo senza autorizzazione, danneggia, commette abusi, illeciti civili o penali nei confronti dell'Ateneo, degli Enti con esso convenzionati o dei terzi che vengono raggiunti, anche sull'Internet, a seguito di una circostanziata relazione dei Responsabili delle risorse coinvolte, è soggetto ai provvedimenti amministrativi e/o disciplinari previsti dai regolamenti dell'Ateneo, nonché alla denuncia alle autorità competenti previste dalla vigente normativa.

Per ogni evenienza non espressamente riportata nel presente Regolamento si applicano le norme previste dai codici civile e penale. Eventuali ricorsi degli interessati non sospendono l'efficacia dei provvedimenti comminati.

Le spese derivanti da eventuali danni causati da un uso improprio delle apparecchiature sono a carico dell'utente.

#### **10.0 Norme transitorie e finali**

Il presente Regolamento viene aggiornato, su proposta del Comitato per la sicurezza informatica, ogniqualvolta le mutate esigenze dell'Ateneo o le innovazioni tecnologiche lo impongano, e comunque almeno ogni due anni, conformemente ai periodici aggiornamenti della normativa sulle misure minime di sicurezza.

L'Ateneo mette a disposizione le risorse per l'attuazione del Regolamento e per la formazione permanente del personale, in particolare quello addetto alla gestione della sicurezza e dei servizi di rete, in misura e secondo modalità deliberate dagli Organi Accademici sulla base delle esigenze e degli sviluppi tecnologici del settore.

Per quanto non esplicitamente previsto e disciplinato dal presente Regolamento, si rinvia alle vigenti norme di legge, allo Statuto, alla normativa internazionale, alle norme del GARR e agli usi in quanto applicabili.