



# UNIVERSITA' DEGLI STUDI DI PAVIA

## Area Sistemi Informativi

Decreto n. 383/2010

**OGGETTO:** Emanazione "Regolamento per l'utilizzo delle risorse informatiche e telefoniche"

PROT. N.

11507

TITOLO: I

CLASSE: 3

### IL RETTORE

**vista** la Deliberazione del Garante in materia di Protezione dei Dati Personali del 01/03/2007: "Lavoro: le linee guida del Garante per posta elettronica e internet" pubblicata sulla Gazzetta Ufficiale N. 58 del 10/03/2007;

**vista** la Deliberazione del Garante in materia di Protezione dei Dati Personali N. 23 del 14/06/2007: "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto in ambito pubblico" pubblicata sulla Gazzetta Ufficiale N. 161 del 13/07/2007;

**vista** la Direttiva della Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica N. 2/2009 del 26/05/2009: "Utilizzo di internet e della casella di posta elettronica istituzionale sul posto di lavoro", che sollecitava le Pubbliche Amministrazioni a fornire ai dipendenti precise indicazioni sull'utilizzo delle risorse informatiche e telefoniche messe a loro disposizione;

**visto** il parere favorevole espresso dalla Delegazione Sindacale nella seduta di contrattazione decentrata del 22/10/2009;

**vista** la Delibera del Consiglio di Amministrazione Repertorio N. 302/2009 del 24/11/2009 relativa all'adozione del "Regolamento per l'utilizzo delle risorse informatiche e telefoniche";

### DISPONE

l'Università di Pavia adotta, a far tempo dal presente decreto, il "Regolamento per l'utilizzo delle risorse informatiche e telefoniche" nella forma approvata nella seduta del Consiglio di Amministrazione del 24/11/2009.

Pavia, 23/3/2010

IL RETTORE  
(Prof. Angiolino STELLA)



**UNIVERSITA' DEGLI STUDI DI PAVIA**

REGOLAMENTO PER L'UTILIZZO DELLE RISORSE  
INFORMATICHE E TELEFONICHE

**Approvato dal Consiglio di Amministrazione in data 24/11/2009**

## SOMMARIO

|          |                                                                                                       |           |
|----------|-------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>SCOPI</b> .....                                                                                    | <b>1</b>  |
| <b>2</b> | <b>APPLICAZIONI</b> .....                                                                             | <b>1</b>  |
| <b>3</b> | <b>DEFINIZIONI</b> .....                                                                              | <b>1</b>  |
| <b>4</b> | <b>REGOLE PER L'ACCESSO, L'UTILIZZO E LA SICUREZZA DELLE RISORSE INFORMATICHE E TELEFONICHE</b> ..... | <b>3</b>  |
|          | 4.1 CRITERI GENERALI .....                                                                            | 3         |
|          | 4.2 UTILIZZO DI SERVER E POSTI DI LAVORO .....                                                        | 3         |
|          | 4.3 UTILIZZO DELLA RETE INTRANET/INTERNET E DEI RELATIVI SERVIZI .....                                | 3         |
|          | 4.4 POSTA ELETTRONICA .....                                                                           | 4         |
|          | 4.4.1 <i>PREMESSA</i> .....                                                                           | 4         |
|          | 4.4.2 <i>AMBITO DI APPLICAZIONE</i> .....                                                             | 5         |
|          | 4.4.3 <i>CONDIZIONI GENERALI</i> .....                                                                | 5         |
|          | 4.4.4 <i>CONDIZIONI SPECIFICHE</i> .....                                                              | 7         |
|          | 4.4.5 <i>USO CONSENTITO</i> .....                                                                     | 8         |
|          | 4.4.6 <i>SICUREZZA E RISERVATEZZA</i> .....                                                           | 9         |
|          | 4.4.7 <i>ARCHIVIAZIONE E CONSERVAZIONE</i> .....                                                      | 9         |
|          | 4.5 TRATTAMENTO DEI DATI .....                                                                        | 9         |
|          | 4.6 PROGRAMMI PER ELABORATORE .....                                                                   | 10        |
|          | 4.7 UTILIZZO DEI DISPOSITIVI E DEI SERVIZI TELEFONICI .....                                           | 11        |
| <b>5</b> | <b>RESPONSABILITÀ E CONTROLLI</b> .....                                                               | <b>11</b> |
|          | 5.1 RESPONSABILITÀ INDIVIDUALI .....                                                                  | 11        |
|          | 5.2 CONTROLLO E USO DEI DATI DI ACCESSO E DI UTILIZZO DEI SISTEMI E DEI LOG .....                     | 11        |
| <b>6</b> | <b>SANZIONI E DIRITTO DI DIFESA</b> .....                                                             | <b>12</b> |

## 1 SCOPI

Il presente regolamento definisce le condizioni per l'accesso, l'utilizzo e la protezione delle risorse informatiche e telefoniche dell'Università degli Studi di Pavia, di seguito indicata come Ateneo.

## 2 APPLICAZIONI

Le regole qua enunciate si riferiscono a tutte le risorse informatiche e telefoniche dell'Ateneo e si applicano a tutti i soggetti che le utilizzano.

Rimane in ogni caso inteso che:

- per le risorse informatiche e telefoniche messe a disposizione o date in uso all'Ateneo 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;
- le utilizzazioni delle risorse informatiche e telefoniche dell'Ateneo devono essere conformi a quanto previsto dalle norme vigenti.

## 3 DEFINIZIONI

*Risorse informatiche* - Qualsiasi tipo di hardware, mezzo di comunicazione elettronica, rete di trasmissione dati, software e informazione in formato elettronico di proprietà dell'Ateneo o ad esso concessi in licenza d'uso.

In particolare le risorse informatiche includono:

- sistemi informativi;
- software applicativi;
- software di base e d'ambiente (sistemi operativi, software di rete, sistemi per il controllo degli accessi, data base, packages, utilities, ecc.);
- files e banche dati;
- mainframe, mini, micro, personal computer, notebook, palmari e ogni altro sistema di elaborazione elettronica delle informazioni;
- stampanti, scanner, plotter, apparecchiature per l'archiviazione elettronica dei dati e i relativi supporti di memorizzazione, video terminali, ecc.;

- modem, dispositivi di rete di ogni tipo (concentratori, ripetitori, bridges, routers, switch, gateways, access point wireless, ecc.);
- mezzi trasmissivi per reti locali e per reti geografiche.

*Risorse telefoniche* - Qualsiasi tipo di apparecchio, mezzo di comunicazione elettronica, rete di trasmissione, software e informazione in formato elettronico di proprietà dell'Ateneo o ad esso concessi in uso.

In particolare le risorse telefoniche includono:

- apparecchi telefonici fissi e mobili;
- centralini e relativi software;
- consolle d'operatore;
- collegamenti telefonici interni ed esterni;
- dispositivi per la fonia wireless.

*Dato* - Tutte le informazioni, indipendentemente dal formato, che sono contenute o elaborate da risorse informatiche dell'Ateneo o che sono contenute o elaborate da risorse informatiche di altri soggetti per conto dell'Ateneo.

*Dato personale* - 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.

*Soggetto* - Qualsiasi dipendente dell'Ateneo, di altro Ente, collaboratore, consulente, studente o fornitore di servizi all'Ateneo a qualsiasi titolo.

*Responsabile* - Soggetto che indipendentemente dalla struttura a cui appartiene (Dipartimento, Istituto, Centro, Presidenza, Laboratorio, Biblioteca, ecc.) ha il compito di coordinare risorse umane e tecnologiche nell'ambito di un contesto ben definito.

*Log* - Qualsiasi registrazione delle attività elaborative compiute da un'applicazione che permette di ricostruire le operazioni svolte da un utilizzatore identificato o identificabile.

## **4 REGOLE PER L'ACCESSO, L'UTILIZZO E LA SICUREZZA DELLE RISORSE INFORMATICHE E TELEFONICHE**

### **4.1 CRITERI GENERALI**

Le risorse informatiche e telefoniche dell'Ateneo devono essere utilizzate per l'assolvimento delle finalità proprie dell'Ateneo.

È vietata qualsiasi attività che possa produrre danni alle risorse informatiche e telefoniche dell'Ateneo o che risulti in contrasto con le regole contenute nel presente testo o con le norme vigenti.

Ogni soggetto è tenuto ad 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 e telefoniche; debbono pertanto essere prontamente segnalati furti, danneggiamenti o smarrimenti di tali strumenti.

Ciascun soggetto che operi nell'ambito dell'Ateneo è tenuto ad uniformarsi alle sopraddette prescrizioni.

### **4.2 UTILIZZO DI SERVER E POSTI DI LAVORO**

Nel caso in cui i server o i posti di lavoro contengano dati personali, ad essi devono essere applicate tutte le prescrizioni di sicurezza previste dal Codice sul Trattamento dei dati personale e, in particolare, dal suo Allegato B.

È consentito l'uso di programmi esclusivamente nel pieno rispetto degli obblighi imposti dalla vigente normativa sulla tutela giuridica del software e del diritto d'autore.

L'Ateneo si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema informativo ovvero acquisiti o installati in violazione del presente Regolamento.

### **4.3 UTILIZZO DELLA RETE INTRANET/INTERNET E DEI RELATIVI SERVIZI**

Ogni utilizzatore della rete è tenuto ad adottare le necessarie misure per non interferire nel corretto funzionamento delle comunicazioni e per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti.

L'accesso e l'uso di risorse informatiche esterne all'Ateneo e da essa non dipendenti è soggetto, nel rispetto del vigente ordinamento, alle norme e regolamentazioni fissate dei titolari di tali risorse.

Non è consentito:

- navigare in siti non pertinenti rispetto alle specifiche necessità di lavoro o di studio, soprattutto se idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché a rivelare lo stato di salute e la vita sessuale;
- lo scarico con procedure non legali di opere protette dal diritto d'autore e da altri diritti connessi al suo esercizio quali opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia, qualunque ne sia il modo o la forma di espressione;
- lo scarico con procedure non legali di programmi per elaboratore tutelati ai sensi della convenzione sulla protezione delle opere letterarie e artistiche, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore;
- la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- qualsivoglia attività vietata dalle leggi vigenti.

Delle navigazioni effettuate in Internet/Intranet viene tenuta traccia solo per le postazioni non custodite e per quelle che fruiscono dell'accesso al servizio tramite rete wireless.

Le copie di sicurezza delle registrazioni del traffico (file di log) delle consultazioni, contenenti la data, l'ora e gli estremi identificativi dell'utilizzatore e delle pagine Web visualizzate, effettuate per fini strettamente correlati alla gestione tecnica del servizio, sono conservate per un massimo di 60 giorni.

#### **4.4 POSTA ELETTRONICA**

##### **4.4.1 PREMESSA**

L'Ateneo fornisce una casella di posta elettronica a tutti i dipendenti e agli studenti. Al personale in quiescenza viene mantenuta la casella istituzionale. La fornitura del servizio ad altri soggetti è sottoposta ad autorizzazione.

Nella definizione delle regole d'uso del servizio di posta elettronica e delle modalità di controllo, l'Ateneo ritiene di grande importanza salvaguardare la libertà di espressione e di pensiero e la garanzia della privacy dell'individuo.

Le condizioni contenute in questo documento valgono anche come informativa sulle finalità e modalità del trattamento dei dati personali, ricavabili dalle attività di controllo

tecnico svolte sul servizio di posta elettronica, ai sensi dell'art. 13 della legge 196/2003.

#### 4.4.2 AMBITO DI APPLICAZIONE

Le regole qua espresse si applicano:

- a tutti i sistemi e i servizi di posta elettronica dell'Ateneo;
- indifferentemente ai contenuti dei messaggi di posta e alle informazioni transazionali (header dei messaggi, indirizzi di posta, dati dei destinatari e dei mittenti) relative a tali messaggi;
- agli amministratori e fornitori di tali servizi;
- tutti gli utenti dotati di una casella di posta elettronica, definiti nei domini appartenenti all'Ateneo;
- a ogni altra categoria di personale come ad esempio fornitori, consulenti, stagisti ecc. cui venga fornito in modo temporaneo un account di posta elettronica per lo svolgimento delle proprie attività;
- a tutti i messaggi di posta elettronica e alle altre registrazioni a questi connesse (indirizzi di posta elettronica, liste di distribuzione, notifiche e log dei messaggi, ecc.) in possesso di dipendenti o di altri utenti, amministratori o gestori del servizio di posta elettronica dell'Ateneo.

#### 4.4.3 CONDIZIONI GENERALI

##### *Finalità del servizio di posta elettronica*

L'Ateneo incoraggia l'uso della posta elettronica per scambiare informazioni, migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro a supporto della missione istituzionale dell'Università.

##### *Proprietà dell'Ateneo*

Il servizio di posta elettronica dell'Ateneo, erogato in proprio o per il tramite di fornitori dei servizi in outsourcing, è di proprietà dell'Università degli Studi di Pavia. Pertanto ogni casella di posta elettronica associata all'Ateneo o a sue articolazioni organizzative o assegnata a individui o funzioni dell'Ateneo, sono di proprietà dell'Università.

##### *Limitazioni di Responsabilità per l'Ateneo*

L'Ateneo non può essere ritenuto responsabile per qualsiasi danno, diretto o indiretto, arrecato all'utente ovvero a terzi e derivante:

- dall'eventuale interruzione del servizio;



- dall'eventuale smarrimento di messaggi diffusi per mezzo del servizio;
- da messaggi inviati/ricevuti o da transazioni eseguite tramite il servizio;
- da accesso non autorizzato ovvero da alterazione di trasmissioni o dati dell'utente.

*Restrizioni all'uso del servizio*

Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè rispettando le leggi, la presente e altre regole e procedure dell'Ateneo e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale.

L'accesso ai servizi di posta elettronica può essere totalmente o parzialmente limitato dall'Ateneo, senza necessità di assenso da parte dell'utente e anche senza preavviso:

- quando richiesto dalla legge e in conformità ad essa;
- in caso di comprovati motivi che facciano ritenere la violazione delle presenti regole o delle disposizioni di legge vigenti;
- al venir meno delle condizioni in base alle quali si ha diritto di utilizzare il servizio;
- in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

*Assenso e conformità*

L'Ateneo è tenuto in generale ad ottenere l'assenso del titolare della casella di posta elettronica prima di ogni ispezione dei messaggi o accesso alle registrazioni o ai messaggi di posta elettronica, fatta eccezione per quanto disposto al successivo punto. D'altro canto, ci si attende che il personale dell'Ateneo soddisfi le richieste dello stesso riguardanti la fornitura di copie delle registrazioni di posta elettronica in suo possesso che riguardino le attività lavorative dell'Ateneo o richieste per soddisfare obblighi di legge, indipendentemente dal fatto che tali registrazioni risiedano o meno su computer di proprietà dell'Università. Il mancato rispetto di tali richieste può portare all'applicazione delle condizioni di cui al punto successivo.

*Limitazioni di accesso senza assenso*

L'Ateneo non ispeziona e non accede ai messaggi di posta elettronica dell'utente senza la sua autorizzazione. L'Ateneo potrà però permettere l'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, anche senza l'assenso del titolare, nei seguenti casi:

- su richiesta scritta dell'autorità giudiziaria nei casi previsti dalla normativa vigente;
- previo preavviso all'utente, per gravi e comprovati motivi che facciano credere che

siano state violate le disposizioni di legge vigenti o le regole dell'Ateneo in materia di sicurezza;

- in situazioni critiche e di emergenza.

#### *Registro elettronico*

L'Ateneo può registrare e conservare i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime: mittente del messaggio, destinatario/i, giorno ed ora dell'invio e esito dell'invio. I file di registro sono conservati per un periodo massimo di sessanta giorni.

#### 4.4.4 CONDIZIONI SPECIFICHE

Gli utenti del servizio di posta elettronica sono avvisati del fatto che:

- la natura stessa della posta elettronica la rende meno sicura di quanto si possa immaginare. Ad esempio, i messaggi di posta elettronica spediti ad una persona possono essere facilmente inoltrati ad altri destinatari. L'Ateneo non può proteggere gli utenti da fatti come quelli descritti che esulano dalle proprie possibilità e compiti. Gli utenti pertanto devono esercitare la massima cautela nell'uso della posta elettronica per comunicare informazioni riservate o dati sensibili;
- i messaggi di posta elettronica, creati e conservati sia su apparati elettronici forniti dall'Ateneo che su altri sistemi, possono costituire registrazioni di attività svolte dall'Università (ricezione o invio di informazioni scambiate tra uffici e personale dell'Ateneo, tra l'Università e enti o società esterne o singoli cittadini). È possibile quindi che venga richiesto di accedere ai contenuti dei messaggi per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Ateneo. L'Università non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge quali la privacy ed altre normative applicabili. Gli utenti devono però tener presente che, per quanto detto, in nessun caso l'Ateneo può garantire che non vi siano accessi alle informazioni personali degli utenti eventualmente presenti in messaggi di posta elettronica residenti sui sistemi dell'Università;
- l'Ateneo, in generale, non può e non intende porsi come valutatore dei contenuti dei messaggi di mail scambiati, né può proteggere gli utenti dalla ricezione di messaggi che possano essere considerati offensivi. Gli utenti sono comunque fortemente incoraggiati a usare nella posta elettronica le stesse regole di cortesia che adopererebbero in altre forme di comunicazione;
- non c'è garanzia, a meno di utilizzare sistemi di posta certificata, che i messaggi ricevuti provengano effettivamente dal mittente previsto, perché è piuttosto semplice

per i mittenti mascherare la propria identità, anche se ciò costituisce, tra le altre cose, una violazione delle presenti regole. Inoltre i messaggi di posta che arrivano come "inoltrato" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto, in caso di dubbi, chi riceve un messaggio di posta elettronica dovrebbe verificare con il mittente l'autenticità delle informazioni ricevute.

#### 4.4.5 USO CONSENTITO

L'uso del servizio di posta elettronica dell'Istruzione è soggetto alle seguenti condizioni.

##### *Proibizioni*

È fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione dell'Ateneo. È inoltre vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali e la fornitura (gratuita o a pagamento) a persone fisiche o giuridiche di qualsiasi lista o elenco degli Utenti del servizio. È proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi e-mail che facciano richiesta di questo tipo di informazioni.

##### *Uso Personale*

È consentito l'utilizzo ragionevole dei propri account nei domini dell'Ateneo a fini privati e personali, purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo non: (i) sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica; (ii) sia causa di oneri aggiuntivi per l'Ateneo; o (iii) interferisca con le attività lavorative dell'utente o con altri obblighi dello stesso verso l'Università. L'utente è edotto del fatto che l'Ateneo considererà, ai fini di eventuali ispezioni, tutti i messaggi di posta elettronica da lui gestiti come strettamente afferenti all'uso del servizio per scopi di lavoro. L'Ateneo presuppone quindi che l'utente decida di utilizzare la posta elettronica per scopi personali avendone preliminarmente e attentamente valutato l'opportunità. Si ricorda comunque che per gli usi personali è possibile dotarsi di una casella di posta elettronica alternativa, ottenibile gratuitamente presso molti fornitori esterni, e liberamente consultabile via internet.

##### *Caselle postali personali e caselle di servizio*

Ove sussista la necessità di garantire il regolare svolgimento di attività lavorative o di studio è consentito rendere disponibili anche indirizzi condivisi (caselle di servizio) tra più soggetti, rendendo così chiara la natura non privata della corrispondenza.

In assenza dei titolari delle caselle di posta è opportuno che vengano attivati meccanismi per l'inoltro di messaggi di risposta automatica con le coordinate di altri

soggetti a cui rivolgersi.

In caso di assenza prolungata o non prevista di un soggetto titolare di una casella postale personale e di improrogabili necessità legate all'attività lavorativa o di studio, il responsabile può autorizzare l'accesso alla corrispondenza elettronica del soggetto assente documentando su un apposito registro le specifiche necessità tecniche/organizzative che hanno motivato l'intervento. Del fatto viene data informazione all'interessato.

#### **4.4.6 SICUREZZA E RISERVATEZZA**

I messaggi di posta elettronica possono essere soggetti ad un esame automatico da parte di software anti-virus e anti-spam; quelli rilevati infetti o indesiderati possono essere bloccati.

Gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la necessità di analizzare i dati transazionali dei messaggi di posta per garantire il corretto funzionamento del servizio e in queste occasioni è possibile che avvengano inavvertitamente accessi al contenuto stesso dei messaggi. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora di verificassero i casi citati.

L'Ateneo si pone come obiettivo fondamentale la fornitura di servizi di posta elettronica sicuri ed affidabili, anche avvalendosi di fornitori altamente qualificati. Va comunque ricordato che la sicurezza e riservatezza della posta elettronica non possono essere garantite in ogni circostanza, in particolare per quanto concerne i messaggi di posta scaricati sui Personal Computer. In questo caso è indispensabile che l'utente stesso provveda ad attuare le azioni adeguate a proteggere le informazioni usando tutti i mezzi disponibili, quali ad esempio password di accesso alle applicazioni e alla propria postazione di lavoro.

#### **4.4.7 ARCHIVIAZIONE E CONSERVAZIONE**

Il servizio di posta elettronica dell'Ateneo prevede il backup dei supporti di memorizzazione contenenti i messaggi solo ai fini di garantire l'integrità e continuità di erogazione del servizio, non per consentire il recupero di messaggi di posta elettronica andati perduti. Pertanto il servizio non prevede la possibilità per l'utente di richiedere assistenza per tale scopo, anche se in casi particolari ciò potrà essere effettuato come forma di cortesia.

### **4.5 TRATTAMENTO DEI DATI**

Qualsiasi dato è un bene dell'Ateneo, deve pertanto essere protetto da distruzioni o perdite anche accidentali, alterazioni, usi illeciti e divulgazioni non autorizzate.

Qualsiasi dato non espressamente rilasciato con strumenti finalizzati alla diffusione pubblica di informazioni è da intendersi riservato.

L'accesso e l'utilizzo di qualsiasi dato riservato deve essere espressamente autorizzato dal Responsabile del dato medesimo.

In particolare i dati personali devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi e utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Ai dati personali devono essere applicate tutte le prescrizioni di sicurezza previste dal Codice sul Trattamento dei dati personali e, in particolare, dal suo Allegato B.

#### **4.6 PROGRAMMI PER ELABORATORE**

Qualsiasi software, a qualsiasi titolo acquisito o realizzato dall'Ateneo, deve essere protetto da distruzioni o perdite anche accidentali, alterazioni, usi illeciti e divulgazioni non autorizzate.

Qualsiasi software non espressamente rilasciato con strumenti finalizzati alla diffusione pubblica è da intendersi riservato.

La riproduzione, installazione, duplicazione, distribuzione e ogni altra forma di utilizzo dei programmi per elaboratore, in quanto opere dell'ingegno tutelate dalla legge, può avvenire lecitamente solo nel rispetto dei diritti d'autore e delle licenze d'uso.

La distribuzione gratuita di software da parte di unità operative dell'Ateneo 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'Ateneo 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'Ateneo 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.

#### **4.7 UTILIZZO DEI DISPOSITIVI E DEI SERVIZI TELEFONICI**

Ogni utilizzatore dei dispositivi e dei servizi telefonici è tenuto ad adottare le necessarie misure per non interferire nel corretto funzionamento delle comunicazioni e per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti.

I dispositivi e i servizi telefonici sono strumenti di lavoro, per cui non è consentito:

- utilizzarli per motivi non attinenti allo svolgimento delle mansioni assegnate;
- inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

## **5 RESPONSABILITÀ E CONTROLLI**

### **5.1 RESPONSABILITÀ INDIVIDUALI**

I soggetti che utilizzano risorse informatiche e telefoniche devono rispettare le regole fissate in questo testo e in particolare:

- mantenere una adeguata riservatezza dei dati;
- 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.

### **5.2 CONTROLLO E USO DEI DATI DI ACCESSO E DI UTILIZZO DEI SISTEMI E DEI LOG**

L'Ateneo intende utilizzare i dati relativi agli accessi ai propri sistemi informatici e telefonici, applicazioni, programmi, dati e transazioni da parte dei componenti la comunità universitaria:

- per motivi di sicurezza;
- per la corretta gestione degli stessi dati e delle informazioni;
- per la corretta gestione delle risorse informatiche e telefoniche;

- per le statistiche d'uso relative ai sistemi informatici e telefonici;
- per le attività relative a modifiche tecniche/operative;
- per l'addebito dei costi relativi agli utilizzi informatici/telefonici alle strutture autonome.

Tali accessi avverranno in conformità con le disposizioni del Garante per la Protezione dei Dati Personali e in particolare delle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)".

Nel pieno rispetto delle previsioni dell' art. 4, comma 2, della L. 300/70, i dati raccolti relativi agli accessi ai servizi informatici/telefonici non saranno in alcun caso utilizzati per controlli inerenti l'attività svolta dagli utilizzatori, né per fini diversi da quelli dichiarati nel presente regolamento.

Esulano da ciò i trattamenti imposti da norme di legge nazionali e internazionali, nonché i trattamenti difensivi derivanti da comportamenti penalmente sanzionati.

## **6 SANZIONI E DIRITTO DI DIFESA**

Il personale che contravviene alle norme indicate nel presente documento, stanti le responsabilità individuali di tipo civile e penale verso terze parti offese, potrà essere oggetto di sanzioni di tipo amministrativo la cui entità e modalità di erogazione saranno definite secondo le procedure previste dai contratti di lavoro attualmente vigenti.

Effettuata la contestazione, immediatamente dopo, il materiale derivante dalla procedura di controllo sarà messo a disposizione dell'interessato ai fini dell'esercizio del diritto di difesa.