REGOLAMENTO IN MATERIA DI UTILIZZO DELLA POSTA ELETTRONICA E DELLA RETE INTERNET MESSI A DISPOSIZIONE DALL'UNIVERSITÀ DI TRIESTE

CONSIGLIO AMMINISTRAZIONE	27/4/2010;
DECRETO RETTORALE	735/2010 dd. 3/6/2010
UFFICIO COMPETENTE	Uff. di Staff Affari Generali e Documentali - Servizio Gestione documentale, privacy e dell'innovazione digitale

Data ultimo aggiornamento **3 giugno 2010** *a cura dell'Ufficio di Staff Affari Generali e Documentali*

Art. 1 - Caratteri generali

Il presente regolamento ha per oggetto i criteri e le modalità operative di accesso e utilizzo del servizio internet e del servizio di posta elettronica da parte del personale dell'Università degli Studi di Trieste, nonché di tutti gli altri soggetti che a vario titolo utilizzano i medesimi servizi.

Il regolamento è adottato sulla base della Legge 20 maggio 1970 n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento", del Decreto Legislativo del 23 giugno 2003 n. 196, recante "Codice in materia di protezione dei dati personali" e secondo le indicazioni contenute nella deliberazione 1 marzo 2007 n. 13 del Garante per la protezione dei dati personali, recante "Linee guida del Garante per posta elettronica e internet".

Art. 2 – Architettura generale dei servizi di rete

La rete telematica dell'Università di Trieste fa parte dell'infrastruttura di rete "GARR - La Rete Italiana dell'Università e della Ricerca Scientifica", della quale utilizza i servizi di collegamento e di interoperabilità.

In tal senso, l'utilizzo della rete di Ateneo è subordinato al rispetto, oltre che del presente Regolamento, anche delle norme dettate dagli organi di governo del GARR che fanno, pertanto, parte integrante del presente Regolamento.

Art. 3 – Utilizzo della rete

Al fine di porre in essere un uso regolare della rete dell'Università di Trieste, gli utenti abilitati sono tenuti a:

- non fornire a soggetti non autorizzati all'accesso il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing (connettere alla rete di Ateneo macchine di terze parti), di hosting (inserire nei server contenuti di terze parti) e simili, salvo approvazione del Nucleo di Sicurezza dell'Ateneo;
- non utilizzare servizi o risorse di rete in un modo che danneggi, molesti o perturbi le attività di altre persone e/o i loro sistemi informatizzati;
- non utilizzare servizi o risorse di rete per finalità che non rientrino in quelle istituzionali connesse al lavoro, allo studio, alla didattica o alla ricerca;
- non creare o trasmettere immagini, dati o altri materiali offensivi, diffamatori, osceni, indecenti, o che attentino alla dignità umana, specialmente se fondati su elementi idonei a discriminare in base al sesso, la razza, la lingua, la religione, le opinioni politiche, le condizioni personali e sociali;
- non trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming") o permettere che le proprie risorse siano utilizzate da terzi per questa attività.

La responsabilità che può sorgere dalla produzione o diffusione, attraverso la rete, di determinati materiali grava sui soggetti che li producono o ne consentono colpevolmente la diffusione.

Il download di file e/o e la loro conservazione su server dell'Ateneo è legittimo solo se effettuato in relazione con l'attività istituzionale.

Art. 4 – Autorizzazioni e credenziali di accesso

Ciascun utente accede alla rete di Ateneo e alle sue risorse utilizzando delle credenziali, consistenti in un codice identificativo (userid) e una parola chiave segreta (password).

La password deve possedere una lunghezza minima di otto caratteri alfanumerici.

Per una corretta pratica di gestione delle password:

- i caratteri alfanumerici che compongono la password non devono formare parole di senso compiuto, e/o significati facilmente riconducibili alla "sfera privata esteriore" dell'utente corrispondente (ad es. data di nascita, nome parenti, indirizzo...);
- è necessario modificare periodicamente la password (ad un intervallo comunque non superiore ai sei mesi, ridotti a tre nel caso di trattamento di dati sensibili), evitando di riutilizzare le password già recentemente impostate.

Il mancato rispetto dei criteri per una corretta gestione della password è un comportamento idoneo a integrare la responsabilità dell'utente in caso di intrusioni da parte di terzi all'interno delle risorse di rete.

Le credenziali sono strettamente personali e non cedibili ad alcuno nella conoscenza o nell'uso (ivi incluso il personale che gestisce i servizi).

Art. 5 – Utilizzo della posta elettronica

L'utilizzo del servizio di posta elettronica è consentito esclusivamente per ragioni di comunicazione di servizio e istituzionali.

È fatto divieto di utilizzare la posta elettronica per diffondere, anche tramite collegamenti ipertestuali o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice eseguibile, ecc.), messaggi che contengano o rimandino a:

- pubblicità non istituzionale, manifesta od occulta;
- comunicazioni commerciali private;
- materiale pornografico o che possa comportare una violazione della Legge 3 agosto 1998 n. 269 "Norme contro lo sfruttamento sessuale dei minori degli anni 18";
- materiale discriminante o lesivo in relazione a razza, sesso, religione;
- materiale che violi la normativa in materia di protezione dei dati personali;
- contenuti o materiali che violino i diritti d'autore di terzi;
- altri contenuti illegali.

In nessun caso gli utenti potranno utilizzare la posta elettronica per diffondere codici dannosi per i computer, quali virus e simili.

Le ordinarie caselle di posta elettronica debbono essere utilizzate esclusivamente per l'invio di testi o altro materiale allegato di dimensione limitata, secondo le indicazioni fornite dalla Divisione Infrastrutture e Servizi Informativi (ISI), in particolar modo qualora siano coinvolti nodi esterni al comprensorio universitario.

L'informazione circa le dimensioni massime dei messaggi trasmissibili, tramite le caselle ordinarie, è reperibile presso la pagina web della Divisione ISI.

Presso la medesima pagina web è disponibile, all'utilizzo degli utenti, apposito servizio per l'invio di file di grandi dimensioni.

Art. 6 – Assenze temporanee / cessazione del rapporto dell'intestatario della casella – personale dipendente

Per il caso di assenze, programmate o prevedibili, del personale dipendente di Ateneo si dispone l'implementazione di funzionalità che consentano l'invio automatico di messaggi, contenenti i recapiti di un altro soggetto o altre utili modalità di contatto della struttura.

In caso di assenze non programmate e non prevedibili, perdurando l'assenza oltre un determinato limite temporale, il responsabile della struttura può disporre lecitamente, sempre che sia necessario e mediante personale incaricato, l'attivazione di un analogo accorgimento, avvertendo il titolare della casella.

Qualora, in caso di assenza non programmata o prolungata, per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto di messaggi di posta elettronica, l'interessato dovrà delegare un altro lavoratore a verificare il contenuto dei messaggi e a inoltrare quelli rilevanti per l'attività lavorativa.

Prima della cessazione del rapporto con l'Ateneo, è fatto obbligo al titolare della casella di trasmettere al responsabile dell'unità organizzativa le e-mail rilevanti per il prosieguo dell'attività istituzionale della medesima.

E' demandata al titolare del trattamento dei dati, la responsabilità di autorizzare, a fronte di gravi e giustificati motivi, l'accesso alle caselle di posta di personale deceduto o irrintracciabile.

In tal caso l'accesso, per il quale andrà stilato apposito verbale, dovrà essere effettuato dal responsabile dell'unità organizzativa di riferimento.

Art. 7 – Mantenimento del diritto di accesso ai servizi

L'accesso ai servizi informatici cessa al termine del rapporto con l'Ateneo.

La casella di posta, dietro richiesta motivata del titolare della casella e autorizzazione del responsabile dell'unità organizzativa, può essere mantenuta attiva per ulteriori sei mesi.

Tale termine può essere superato nel caso in cui il titolare del rapporto cessato mantenga con l'Ateneo, in qualunque forma, un rapporto di collaborazione.

E' possibile, a richiesta dell'interessato, mantenere l'iscrizione nelle liste di posta generali dell'Ateneo per consentire l'informazione anche del personale cessato sulle iniziative comuni di Ateneo.

In tal caso l'interessato dovrà comunque indicare l'indirizzo e-mail personale cui dette comunicazioni dovranno essere inviate.

Eventuali pagine web personali, ospitate tra le risorse web di Ateneo e legate ad attività di didattica o ricerca possono essere mantenute, in base a richiesta motivata dell'autore e autorizzata dal responsabile della struttura, fintantoché sia giustificata la loro pubblicazione.

Art. 8 – Riservatezza ed integrità della posta elettronica

L'Università tutela la riservatezza e l'integrità dei messaggi di posta elettronica diretti alle caselle personali durante il loro transito e la loro permanenza nel sistema di posta.

Per il raggiungimento di tale obiettivo, l'Università si avvale di strumenti idonei a verificare, mettere in quarantena e cancellare, anche senza alcun avviso agli utenti, i messaggi che potrebbero compromettere il buon funzionamento del servizio, in quanto risultati positivi ai test antivirus o altro codice malevolo.

Art. 9 – Rispetto della normativa sul trattamento dei dati personali

Ai sensi di quanto disposto dalla vigente legislazione in materia di privacy, sono sottoposte a crittografia le informazioni contenenti dati sensibili, prima del loro invio tramite posta elettronica.

I responsabili delle strutture didattiche, scientifiche e di servizio dell'Ateneo hanno l'obbligo di comunicare tempestivamente gli elaboratori sui quali risiedono banche dati contenenti dati personali e/o sensibili, al fine di un puntuale adempimento di quanto previsto dalla normativa in tema di misure minime e idonee di sicurezza.

Devono essere adottati opportuni strumenti di protezione dei dati memorizzati su dispositivi mobili (palmari, notebook, smartphone, penne USB, dischi rigidi esterni, schedine SD, etc).

Art. 10 – Trattamento dati di accesso

L'Università può avvalersi di sistemi di controllo che hanno la finalità di garantire la sicurezza nel trattamento dei dati e nell'uso della dotazione informatica.

Le attività sull'uso del servizio di accesso a internet sono automaticamente registrate in forma elettronica nel rispetto delle disposizioni di legge in materia e automaticamente cancellate in base alla normativa vigente.

Esse sono conservate presso la Divisione ISI o, in alternativa, presso le strutture che gestiscono gli elaboratori su cui risiedono i servizi.

I dati personali contenuti nei log sono oggetto di trattamento esclusivamente nelle seguenti ipotesi:

- per rispondere ad eventuali richieste della polizia delle comunicazioni e/o dell'autorità giudiziaria;
- per l'erogazione del servizio;
- per l'analisi di malfunzionamenti;

- per l’effettuazione di statistiche sull’utilizzo delle risorse, previa anonimizzazione degli stessi.

Al fine di assicurare il rispetto delle norme e del regolamento relativo all’utilizzo della rete, anche in virtù di quanto stabilito dall’art. 8 comma 3 del Regolamento “Accesso al Sistema Integrato di Reti dell'Ateneo” (SIRA), il personale della Divisione ISI, d’intesa con il responsabile della struttura, adotta tutte le misure necessarie, compresa l’effettuazione di controlli con idonei software sul traffico in rete.

Le partizioni organizzative dell’Ateneo che attivino servizi che trattino o che permettano il trattamento di informazioni di carattere personale dei lavoratori, devono rendere nota, a richiesta del lavoratore, l'identità degli amministratori di sistema.

Art. 11 – Sanzioni

La violazione delle norme disposte dal presente Regolamento comporta la revoca o la limitazione (temporanea o permanente) delle autorizzazioni ad accedere alle risorse informatiche gestite dall'Università, fatte salve le altre sanzioni previste dalle norme vigenti.