UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

REGOLAMENTO PER L'ACCESSO, L'UTILIZZO E LA PROTEZIONE DELLE RISORSE INFORMATICHE

1. Premesse

Il presente regolamento definisce le condizioni per l'accesso, l'utilizzo e la protezione delle risorse informatiche dell'Università degli Studi di Bari - Aldo Moro, di seguito indicata come Ateneo.
L'Ateneo, consapevole delle potenzialità offerte dagli strumenti informatici e telematici, promuove l'utilizzo della Rete Dati di Ateneo, quale strumento utile, sempre compatibilmente con le proprie strutture e risorse, esclusivamente a perseguire le proprie finalità nel quadro dell'attività istituzionale e amministrativa, della didattica, della ricerca e della terza missione.

2. Finalità e ambito di Applicazione

Le risorse informatiche costituiscono strumenti indispensabili per l'Università, in quanto consentono l'accesso, l'elaborazione e la distribuzione dell'informazione e della conoscenza sviluppate all'interno e all'esterno di essa. L'Università pertanto concede in uso ai docenti, al personale tecnico amministrativo, ai collaboratori ed esperti linguistici, nonché agli studenti apparecchiature informatiche di proprietà dell'Università e ne promuove l'utilizzo, ritenendole strategiche per le attività didattiche, scientifiche ed amministrative.
Poiché tali tecnologie potenziano le capacità individuali all'accesso, alla copia, all'analisi ed alla rielaborazione delle informazioni, gli utenti devono essere consapevoli dei limiti che ne configurano un uso appropriato, nel rispetto della normativa in materia di privacy.
Gli utenti delle risorse di elaborazione dell'Università sono tenuti a farne uso corretto, ad averne cura e ad utilizzarle per i soli scopi istituzionali per l'assolvimento delle proprie finalità, anche al fine di prevenire o minimizzare i rischi di incidente informatico.

Il presente regolamento si applica a tutte le risorse informatiche dell'Ateneo e a tutti i soggetti che le utilizzano.

Rimane in ogni caso inteso che:

- per le risorse informatiche messe a disposizione o date in uso all'Ateneo da altri Enti o organizzazioni valgono gli accordi e le condizioni contrattuali stipulate tra le parti;
- per l'utilizzo di dati, programmi e materiali valgono le condizioni di copyright, ove previsto;

- le utilizzazioni delle risorse informatiche dell'Ateneo devono essere conformi a quanto previsto dalle norme vigenti;
- in qualunque momento, in caso di inosservanza del presente regolamento, l'Ateneo ha la facoltà di revocare all'utente qualunque utilizzo delle attrezzature hardware e software ad esso fornite.

3. Definizioni

Centro servizi informatici - struttura preposta alla gestione tecnica dei servizi informatici di Ateneo e gestione delle banche dati ad uso dell'amministrazione centrale, d'ora in poi CSI;

Credenziali di accesso - dati utilizzati nelle operazioni di autenticazione utente (nome utente e password);

PDL - Postazione di Lavoro in cui si presta abitualmente servizio e comprendente, nell'accezione intesa in questo regolamento, un elaboratore elettronico collegato alla Rete informatica di Ateneo.

Firma elettronica qualificata - firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro (ad es.: smart card) per la creazione della firma;

Firma digitale - particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

GARR - Gruppo Armonizzazione Reti per la Ricerca;

Host - ogni computer, stampante, periferica, telefono, fax, smartphone o qualsiasi dispositivo informatico connesso alla Rete Dati;

Indirizzo IP - Numero che identifica univocamente un host nella Rete Dati di Ateneo;

Posta Elettronica Certificata - è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici, d'ora in poi PEC;

Punto Rete - punto di connessione fonia/dati, al quale può essere collegato un host;

Rete dati di Ateneo - insieme di infrastrutture fisiche e logiche che consentono la comunicazione e la trasmissione dati sia all'interno dell'Ateneo che verso l'esterno attraverso la rete di interconnessione gestita dal GARR;

Servizi di Rete - servizi che utilizzano la Rete Dati di Ateneo e che sono erogati da alcune strutture dell'Ateneo per attività dell'amministrazione centrale (U-GOV, Contabilità), della didattica e della ricerca (Esse3), posta elettronica, protocollo informatico (Titulus), servizi di segreteria (Esse3), sistema di rilevazione e gestione presenze (MyAliseo), portale web di Ateneo, servizi di autenticazione e autorizzazione;

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, database, package, utility, ecc.)
- file e banche dati
- mainframe, mini - micro - personal computer, notebook, palmari, smartphone 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, bridge, router, switch, gateway, access point wireless, etc.);
- mezzi trasmissioni per reti locali e per reti geografiche.

Dato - tutte le entità, 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 per la produzione di informazioni e/o conoscenza

Dato personale - qualunque informazione che identifichi o renda identificabile una persona fisica, una persona giuridica, un ente od un'associazione, e che possa fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni, il suo stato di salute, la sua situazione economica, ecc. anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Utente - Qualsiasi dipendente dell'Ateneo, di altro Ente, collaboratore, consulente, studente o fornitore di servizi all'Ateneo a qualsiasi titolo che accede ai servizi di rete dell'Ateneo attraverso la Rete dati di Ateneo;

Responsabile - Soggetto che indipendentemente dalla struttura a cui appartiene (Dipartimento, Centro, 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. Soggetti coinvolti

I soggetti coinvolti per le finalità di cui al presente regolamento sono tutti coloro che rientrano nella definizione di “Utente” di cui all’art. 3.
Ai sensi dello statuto di Ateneo e del CSI i compiti di gestione dei protocolli di accesso del sistema informativo di Ateneo e la gestione dei servizi informatici e telematici di utilità generale per l’Università sono attribuiti al predetto Centro.
Il CSI secondo il proprio statuto (Art. 8) è gestito secondo le modalità stabilite dal “Regolamento di Ateneo per l’amministrazione, la finanza e la contabilità.”

5. Regole per l’accesso e l’utilizzo delle risorse informatiche di Ateneo

5.1 CRITERI GENERALI

Ogni utente 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; devono pertanto essere prontamente segnalati furti, danneggiamenti o smarrimenti di tali strumenti.

Ciascun utente che operi nell’ambito dell’Ateneo è tenuto ad uniformarsi alle sopraddette prescrizioni.

È vietata qualsiasi attività che possa produrre danni alle risorse informatiche dell’Ateneo o che risulti in contrasto con le regole contenute nel presente regolamento o con le nome vigenti in materia.

Gli aspetti relativi alla posta elettronica restano disciplinati dal “Regolamento per l’uso della posta elettronica” emanato con Decreto Rettorale n.

Gli aspetti relativi alla sicurezza informatica restano disciplinati dal “Regolamento per la sicurezza informatica” emanato con Decreto Rettorale n.

5.2 UTILIZZO DI ELABORATORI E POSTAZIONI DI LAVORO

Nel caso in cui gli host o le postazioni di lavoro contengano dati personali, ad essi devono essere applicate tutte le prescrizioni di sicurezza previste dal Codice sul Trattamento dei dati personali (Regolamento U.E. 2016/679 del 27 aprile 2016).

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.
In particolare:

- l’utente è responsabile per le attività svolte nella Rete dati di Ateneo;
- l’utente è responsabile per eventuali difformità riscontrate sulle apparecchiature assegnate;
- la modifica dell’indirizzo IP configurato (in maniera dinamica o manualmente) sull’host assegnato è espressamente vietata;

- le credenziali di accesso alla Rete di Ateneo e ai servizi di Rete di ogni genere sono personali e non possono essere condivise o cedute;
- l'utente è responsabile per la protezione dei dati utilizzati e/o memorizzati nei sistemi a cui ha accesso ed è tenuto ad adottare tutte le misure necessarie ai sensi della normativa vigente e del "Regolamento per la sicurezza informatica" emanato dall'Ateneo;
- la responsabilità dei contenuti prodotti e diffusi attraverso la rete di Ateneo è dell'utente che li produce e li diffonde;
- l'utente è tenuto a segnalare al CSI o al referente di struttura ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
- l'utente è tenuto ad aggiornarsi su direttive di sicurezza o comportamenti da adottare periodicamente diffusi dal CSI attraverso il proprio sito o per mezzo di comunicazioni per posta elettronica in particolare è tenuto a installare e mantenere aggiornato l'eventuale software antivirus sull'Host affidato. Tale antivirus deve necessariamente essere quello acquistato dall'Ateneo per tale scopo. Al fine di schedulare le richieste di supporto al CSI l'utente dovrà utilizzare apposita procedura on line di customer care messa a disposizione del CSI. Nessuna attività di manutenzione all'host sarà garantita in caso di inosservanza della presente disposizione.
- l'utente è tenuto ad impostare ed attivare il blocco con password del sistema operativo in caso di allontanamento anche temporaneo dal videoterminale, al fine di evitare di lasciare la risorsa informatica incustodita;
- l'utente è tenuto a spegnere il proprio host al termine dell'attività lavorativa prima di allontanarsi dalla postazione di lavoro salvo motivate esigenze di servizio/istituzionali. In caso di inosservanza si applicano le sanzioni previste all'art. 7 del presente regolamento.

È vietato:

- utilizzare le risorse hardware e software fornite dall'Ateneo, per conservare file di natura personale per scopi non strettamente correlati con le finalità lavorative;
- accedere alla Rete Dati di Ateneo per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'Università; fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso alla Rete di Ateneo;
- usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi; ove l'utente contravvenga a tale divieto il CSI provvederà ad impedire l'accesso alla Rete;
- violare obblighi in materia di copyright, licenze d'uso di software;
- svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, danneggino o restringano l'utilizzabilità o le prestazioni della Rete di Ateneo.
- Manomettere in qualsiasi modo le apparecchiature e le strutture informatiche ed elettroniche dell'Ateneo;
- violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (software, database, ecc.), intercettare, tentare di intercettare o

accedere a dati in transito sulla Rete Dati d'Ateneo, dei quali non si è destinatari specifici;

- 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;
- diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio o dal contenuto osceno;
- utilizzare la Rete dati di Ateneo e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale;
- trasferire materiale in violazione delle norme sulla proprietà intellettuale, mediante programmi di tipo "Peer to Peer";
- trasferire attraverso la rete documenti (filmati, fotografie, musica o altri documenti multimediali) ad uso strettamente personale anche se muniti di regolare diritto di utilizzo, non inerente la normale attività lavorativa.
- cablare o collegare risorse informatiche ai punti rete senza l'autorizzazione del CSI;
- connettere un Host, contemporaneamente, alla rete d'Ateneo e ad altra rete (es. ADSL, GPRS);
- copiare (a meno che la licenza d'uso non lo consenta) e/o utilizzare i programmi messi a disposizione dall'Amministrazione per installazioni esterne;

L'Ateneo si riserva la facoltà di procedere tramite il CSI alla rimozione di ogni file o applicazione, anche dotati di regolare licenza d'uso, che riterrà essere pericolosi per la sicurezza del sistema informatico o causa di malfunzionamenti per l'host o per la rete dati, ovvero acquisiti o installati in violazione del presente Regolamento.

5.3 UTILIZZO DELLA RETE E DEI RELATIVI SERVIZI

Ogni utilizzatore della rete è tenuto in ogni caso 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.

Non è consentito:

- navigare in siti non pertinenti rispetto alle specifiche necessità di lavoro o di studio;
- il download 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, alla cinematografia, qualunque ne sia il modo o la forma di espressione;
- il download 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 scelta o la disposizione del materiale costituiscono una creazione 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.

Le copie di sicurezza delle registrazioni del traffico (file di log) degli accessi e/o delle applicazioni, contenenti la data, l'ora e gli estremi identificativi dell'utilizzatore, effettuate per fini strettamente correlati alla gestione tecnica del servizio sono conservate secondo le norme di legge.
Per l'utilizzo della rete e dei relativi servizi si applica la disciplina prevista nel Regolamento sulla Sicurezza Informatica.

5.4 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.
Per tutto quanto non espressamente previsto nel presente regolamento in materia di trattamento dei dati si fa rinvio al regolamento sulla privacy.

5.5 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.

Si precisa che:

- l'Ateneo non fornisce alcuna garanzia su software distribuiti gratuitamente e in particolare non garantisce la loro adeguatezza e fruibilità per scopi specifici;
- in nessun caso l'Ateneo potrà essere ritenuto responsabile per danni diretti, indiretti o derivanti dall'uso dei software distribuiti gratuitamente o dai risultati da essi forniti; in particolare non potrà essere ritenuto 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.

6. Responsabilità e controlli

6.1 RESPONSABILITA' E ADEMPIMENTI

I soggetti che utilizzano risorse informatiche devono rispettare il presente regolamento e in particolare:

- mantenere la riservatezza sia dei dati sia delle misure di sicurezza adottate e delle modalità di accesso ai servizi, nel rispetto della normativa in materia;
- utilizzare esclusivamente le risorse alla cui fruizione essi sono abilitati.

Il Centro Servizi Informatici è la struttura tecnica deputata:

- alla gestione dell'infrastruttura di Rete alla quale le Risorse Hardware e Software di proprietà dell'Ateneo vengono collegate;
- alla erogazione di tutti i servizi infrastrutturali e di supporto per lo svolgimento delle attività di didattica, ricerca, terza missione e documentali;
- alla verifica dell'applicazione del presente regolamento;
- alla segnalazione di eventuali violazioni agli organi competenti.

6.2 CONTROLLO E USO DEI DATI DI ACCESSO E DI UTILIZZO DEI SISTEMI E DEI LOG

L'Ateneo utilizza i dati relativi agli accessi ai propri sistemi informatici, 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;
- per le statistiche d'uso relative ai sistemi informatici;
- per le attività relative a modifiche tecniche/operative.

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 rispetto delle previsioni di cui all’art. 4 della L. 300/70, i dati raccolti relativi agli accessi ai servizi informatici saranno utilizzati garantendo la protezione dei dati personali, in conformità con la disciplina legislativa in materia e nella tutela di interessi economici e commerciali vivi, ivi compresi la proprietà intellettuale, il diritto d’autore e i segreti commerciali secondo le specifiche norme nazionali e internazionali vigenti in materia.

6.3 Applicazione del regolamento

Ciascun Centro, Dipartimento, Direzione o altra struttura prevista nel modello organizzativo di Ateneo è tenuta ad individuare uno o più referenti con il compito di curare l'assistenza (hardware e software) all'utenza afferente alla medesima struttura.

In particolare i referenti di struttura rappresentano l’interfaccia amministrativa e tecnica dell’utenza ed a tal fine sono tenuti a curare la distribuzione e/o installazione, nel rispetto delle norme amministrative e tecniche, stabilite caso per caso, dei software licenziati centralmente dal CSI e collaborano all’assistenza tecnico-funzionale degli apparati informatici relativi alla propria struttura.
In nessun caso i referenti dovranno intervenire sulle apparecchiature di rete e sul cablaggio strutturato di propria iniziativa.

7. Sanzioni

A fronte di violazioni accertate delle regole stabilite dal presente regolamento, al fine di evitare ripercussioni sulla Rete Telematica e sui servizi, i responsabili delle Unità Operative del Centro Servizi Informatici, competenti nella materia, possono disporre la sospensione temporanea delle credenziali di identità digitale che consentono la fruizione dei servizi di Ateneo. Detta sospensione deve essere comunicata immediatamente all’interessato e al Gruppo Sicurezza ICT (art. 4.2 del Regolamento per la Sicurezza dei servizi ICT dell’Università degli Studi di Bari Aldo Moro).

Il CSI può disattivare in qualsiasi momento un codice d’accesso personale e/o una password, apparati ritenuti non conformi o pericolosi ai fini della sicurezza, disconnettere un host dalla rete, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all’integrità o al funzionamento della Rete Telematica di Ateneo, oppure qualora vi sia evidenza - che l’utente abbia violato il presente Regolamento.

Il CSI si riserva la possibilità di erogare assistenza in caso di violazione del presente regolamento, ferma restando la segnalazione agli Organi competenti di Ateneo, e le eventuali applicazioni di sanzioni disciplinari, civili per danni e penali.

8. Disciplina di modifica del presente regolamento

Il presente regolamento è approvato dal Consiglio di Amministrazione previo parere del Senato Accademico, su proposta del CTS del CSI, viene emanato con Decreto del Rettore ed entra in vigore il giorno successivo alla pubblicazione sul sito web istituzionale.

Eventuali modifiche e integrazioni al presente regolamento seguiranno la medesima procedura di cui al comma 1.

Sommario