Università degli Studi
Mediterranea
di Reggio Calabria

REGOLAMENTO DI ACCESSO

ALLA RETE DI ATENEO

Art. 1 – Definizioni

1. Ai fini del presente regolamento si intende per:
   - **Ateneo**: L'Università degli Studi Mediterranea di Reggio Calabria in tutte le sue articolazioni istituzionali e territoriali.
   - **Rete d'Ateneo:** L'insieme delle attrezzature, dei cablaggi e degli impianti che consentono il collegamento informatico e telematico tra le diverse strutture e stazioni di lavoro e l'accesso alle reti telematiche esterne.
   - **Utenti:** Tutti coloro che hanno accesso alla Rete d'Ateneo in accordo col presente regolamento.
   - **Identità Informatica**: L'insieme di dati (compresi quelli personali) e di credenziali che vengono associati agli utenti per la loro identificazione sulla Rete di Ateneo.
   - **Utenti Registrati:** gli utenti dell'Ateneo non estemporanei ai quali è stata attribuita una identità informatica, che corrispondono a personale strutturato o collaboratori che a diverso titolo utilizzano le attrezzature dell'Ateneo e che hanno ottenuto l'accesso alla Rete a seguito della procedura prevista dall'At. 9 del presente regolamento.

Art. 2 - Organi di Riferimento

In materia di reti di trasmissione dati gli Organi di riferimento autorevoli nei rispettivi ambiti di intervento sono i seguenti:

- GARR, Gestione e Ampliamento Rete Ricerca (www.garr.it), in particolare l'Organismo Tecnico Scientifico (OTS), di nomina ministeriale, e il Nucleo Tecnico GARR-CRUI.
- Il CESIAT è autorevole per l'accesso alla rete GARR nazionale, per la gestione delle classi di indirizzi IP assegnate all'Ateneo dal GARR-LIR, per la pianificazione, l'aggiornamento, la gestione, il controllo, la sicurezza e la manutenzione dell'infrastruttura di Rete dell'Ateneo e per tutto quanto oltre stabilito dal presente regolamento.

L'Ateneo considera inoltre autorevole in tema di sicurezza informatica il servizio operativo GARR-CERT (www.cert.garr.it) e, in ambito internazionale, il CERT-Computer Emergency Response Team (www.cert.org) dell'Università Carnegie Mellon (USA).

Art. 3 - Oggetto e Ambito di Applicazione

Il presente regolamento si applica a quanti facciano uso delle strutture della Rete di Ateneo. La rete di Ateneo collega permanentemente le diverse sedi in cui si articola l'Ateneo. Essa è interconnessa alla rete GARR e, tramite quest'ultima, alla rete Internet. L'uso delle risorse e dei servizi di Internet tramite la rete d'Ateneo è pertanto subordinato al rispetto da parte degli utenti oltre che del presente regolamento, anche delle norme dettate dagli organi di governo del GARR in ordine all'accesso e all'utilizzo della stessa rete GARR.

Art. 4 – Responsabilità

Ogni utente risponde in pieno delle proprie attività in Internet e sulla Rete Locale delle attività svolte per mezzo della rete. Ciò vale in particolare per le fattispecie di natura civile e penale.
L'Ateneo, nelle sue strutture competenti, adotta tutte le adeguate strategie di monitoraggio dei dati relativi al traffico (escludendo pertanto i contenuti delle comunicazioni) atte a consentire la verifica della responsabilità di eventuali attività illecite svolte attraverso l'uso della Rete di Ateneo, nei casi e con le modalità previste dalla normativa vigente in materia di sicurezza informatica e protezione dei dati personali.
In ogni caso, l'utilizzo della Rete, è strettamente condizionato al rispetto dei divieti espressamente richiamati nel presente regolamento nonché da quelli derivanti dalle norme di carattere generale e specifico in vigore.

Art. 5 - Dati personali

Gli organi competenti dell'Ateneo memorizzano i dati personali degli utenti registrati. Tali dati sono necessari per la gestione dei servizi erogati e gli utenti ricevono regolare informativa prodotta a norma delle leggi in vigore in materia di protezione dei dati personali.

Art. 6 - Principi sulla Sicurezza del Sistema e sul Comportamento degli Utenti

Le attività del singolo utente non possono compromettere lo svolgimento di quelle degli altri utenti. È vietato appesantire il sistema; l'importazione o la trasmissione di grandi quantità di dati dovrebbe essere quindi effettuata al di fuori delle ore di punta. Ciò vale sia per il traffico di dati all'interno della Rete di Ateneo che verso l'esterno. In particolare l'invio di e-mail a tutti gli utenti della rete è di norma effettuato dall'Ufficio Informazione e Comunicazione dell'Ateneo e dal Centro Servizi Informatici di Ateneo (CESIAT), quest'ultimo per le comunicazioni di carattere tecnico.
Gli utenti sono tenuti a comunicare immediatamente qualsiasi caso di abuso e di intervento dall'esterno agli amministratori del sistema, i quali potranno così adottare le necessarie contromisure.
Nello specifico, è vietato qualsiasi tentativo di effettuare un accesso non autorizzato a computer e dati, di sovraccaricare i computer e di sfruttare eventuali lacune nel sistema di sicurezza; è vietato inoltre qualsiasi tipo di intercettazione di trasmissione dati. Tali comportamenti comportano l'estromissione dell'utente dall'uso della rete, e, nei casi in cui si configuri la fattispecie del reato, la denuncia alle autorità competenti.
È severamente proibito sabotare o manipolare hardware o software collocati sul server o su altri computer, come pure sabotare o manipolare apparecchi collegati alla rete come stampanti, scanner ecc.
Gli host della rete devono prevedere meccanismi di autenticazione basati su credenziali informatiche in possesso esclusivo degli utenti autorizzati. I meccanismi di autenticazione utilizzati da tutti gli utenti su host della rete di Ateneo, devono seguire le stesse prescrizioni imposte dalla normativa in vigore in materia di protezione dei dati personali, in riferimento alla loro definizione e gestione. Ciò vale anche relativamente agli obblighi di dotare ogni macchina di adeguati sistemi di protezione contro l'intrusione e l'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
L'Ateneo adotta adeguate misure atte a prevenire l'uso incongruo o illecito della Rete di Ateneo e dei servizi in essa erogati, corrispondenti a:
a) Responsabilizzazione degli utilizzatori finali, attraverso la diffusione dell'informazione circa i rischi penali connessi all'uso indebito del mezzo informatico o alla riproduzione non autorizzata di software.
b) Formazione degli utilizzatori finali, attraverso corsi di introduzione e di aggiornamento, non solo mirati all'aspetto tecnico-applicativo, ma anche alla tematica della sicurezza informatica, in relazione sia al profilo interno della protezione dei dati dell'Ateneo, sia a quello esterno, relativo ai rischi connessi all'accesso a sistemi informatici di terzi.
c) Limitazione degli accessi a sistemi informatici esterni solo agli utilizzatori che ne abbiano effettiva necessità per ragioni di servizio.
d) Meccanismi di controllo e di protezione dei sistemi di rete ed informatici adeguati agli standard tecnologici internazionali.

Art. 7 – Divieti

In aggiunta a quanto stabilito dalle leggi in materia di reati informatici, in accordo ai principi enunciati nell'Art. 6 del presente regolamento, è vietato utilizzare la Rete di Ateneo:
1. in assenza di regolare autorizzazione;
2. per qualsiasi tipo di uso commerciale;
3. in modo difforme dalle regolamentazioni dettate dai responsabili della rete GARR;
4. per scopi incompatibili con le finalità e con l'attività istituzionale dell'Ateneo così come stabilito nello Statuto dell'Università;
5. per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'Ateneo;
6. per commettere attività che violino la riservatezza di altri utenti o di terzi;
7. per attività atte ad influenzare negativamente la regolare operatività della rete, a limitarne l'utilizzabilità o degenerarne le prestazioni;
8. per attività che provochino trasferimenti non autorizzati di informazioni (software, basi dati, etc.);
9. per attività che violino le leggi a tutela delle opere dell'ingegno.

È inoltre tassativamente vietato, in violazione delle misure adottate dall'Ateneo per assicurare la tracciabilità delle attività svolte dagli utenti, usare l'anonimato o servirsi di tecniche mirate ad ottenere l'accesso anonimo o con falsa o indefinita identità informatica alla Rete di Ateneo e ai servizi in essa erogati, ivi compresa la posta elettronica.
In ordine ai divieti, per tutto ciò non espressamente citato, valgono le disposizioni previste dalle leggi in materia di crimini informatici, nonché le leggi vigenti per ciò che attiene responsabilità civile e penale dell'autore di eventuali comportamenti illeciti connessi all'utilizzo della Rete di Ateneo.

Art. 8 - Utenti Estemporanei e Reti Wireless

Qualsiasi Struttura dell'Ateneo, che, o per eventi scientifici o didattici, o per l'espletamento delle finalità connesse all'utilizzo di laboratori o aule informatiche, consenta l'accesso alla Rete ad utenti non registrati, dovrà, in ottemperanza alle leggi in vigore in materia di sicurezza informatica:

a) identificare chi accede ai servizi telematici offerti, prima dell'accesso stesso o dell'offerta di credenziali di accesso, acquisendo i dati anagrafici riportati su un documento di identità, nonché il tipo, il numero e la riproduzione del documento presentato dall'utente;
b) rendere disponibili, a richiesta, i dati acquisiti relativamente all'identificazione degli utenti e al monitoraggio delle attività da essi svolte, esclusi comunque i contenuti delle comunicazioni, al Servizio polizia postale e delle comunicazioni, quale organo del Ministero dell'interno preposto ai servizi di polizia postale e delle comunicazioni, nonché, in conformità al codice di procedura penale, all'autorità giudiziaria e alla polizia giudiziaria;
c) adottare le misure fisiche o tecnologiche occorrenti per impedire l'accesso agli apparecchi terminali a persone che non siano preventivamente identificate.

Le Strutture che, anche temporaneamente, offrono accesso alle reti telematiche utilizzando tecnologia *wireless*, in aree messe a disposizione di utenti non registrati, sono tenute ad adottare le misure fisiche o tecnologiche occorrenti per impedire l'uso di apparecchi terminali che non consentono l'identificazione dell'utente, ovvero ad utenti che non siano identificati secondo le modalità descritte alla lettera a) comma 1 del presente articolo. Le politiche di sicurezza adottate sono comunque soggette al controllo da parte del CESIAT e in accordo con esso definite. Relativamente alla identificazione degli utenti, si applicano le disposizioni previste dall'Art. 10 del presente regolamento.

Art. 9 - Utenti Registrati

1. Possono essere Utenti Registrati, in conformità a quanto previsto nell'Art. 1 del presente regolamento, tutte le unità di personale strutturato dell'Ateneo (*utenti strutturati*), nonché dottorandi, borsisti, collaboratori, contrattisti e "*visiting scholar*" (*utenti non strutturati*).
2. Per ogni utente non strutturato viene individuato, all'interno del personale strutturato, un *Referente Interno*, corrispondente al supervisore nel caso di borsisti o dottorandi, al responsabile del relativo progetto nel caso di contrattisti, ad un docente responsabile nel caso di collaboratori o visiting scholar. Il Referente Interno ha il compito di responsabilizzare l'utente rispetto al corretto utilizzo della Rete di Ateneo, in conformità a quanto previsto dal presente regolamento, e ha le funzioni di riferimento per ogni comunicazione tra Ateneo ed utente inerente all'utilizzo della Rete di Ateneo. E' compito del Referente Interno, altresì, comunicare al CESIAT l'avvenuta conclusione del rapporto di lavoro o del periodo di permanenza dell'utente, in modo da poter procedere alla dismissione dell'utenza stessa. Gli effetti della registrazione, limitatamente al caso di utenti non strutturati, decadono in ogni caso nel termine di 24 mesi dall'attivazione, previa notifica al Referente Interno.
3. La procedura di registrazione dell'utente consiste nell'invio, da parte dell'utente al Direttore del CESIAT, di una domanda, secondo le formalità definite dal CESIAT, nella quale l'utente dichiara di aver preso visione delle disposizioni incluse nel presente regolamento, si impegna ad osservarle e si assume piena responsabilità delle attività svolte attraverso la Rete di Ateneo. La domanda deve essere vistata dal Direttore (o dirigente del settore – Preside, nel caso della Facoltà) della Struttura a cui afferisce, nel caso di utenti strutturati, della Struttura a cui afferisce il suo Referente Interno, nel caso di utenti non strutturati. Limitatamente al caso di utenti non strutturati, alla domanda deve essere allegata fotocopia di un documento di identità valido dell'utente.

Art. 10 - Identificazione degli Utenti e Funzioni Centralizzate

1. In aggiunta a quanto stabilito dagli Artt. 8 e 9 del presente regolamento, l'identità informatica degli utenti è ottenuta attraverso adeguati meccanismi di assegnazione di dati identificativi dell'utenza di rete (IP, indirizzi della scheda di rete, meccanismi basati su credenziali informatiche). Tale funzione è svolta in esclusiva dal CESIAT, salvo quanto previsto nel comma 2 del presente articolo.
2. Eventuali meccanismi di assegnazione locale (NAT/PAT dovuti a presenza di *firewall, proxy*, o installazione di reti *wireless*) che fanno corrispondere i dati identificativi di una utenza di rete a uno o più identificativi di classe privata, mascherando verso l'esterno pertanto la reale identità informatica dell'utilizzatore della Rete di Ateneo relativamente al traffico in uscita dal segmento di rete che adotta tali meccanismi, possono essere messi in atto dalle Strutture dell'Ateneo, solo se preventivamente autorizzate dal CESIAT, dotate di un referente tecnico nominato secondo le formalità previste dall'Art. 11 comma 4 del presente regolamento, e impiegando meccanismi che consentano in ogni momento di tenere traccia della reale identità informatica degli utilizzatori, anche relativamente a precedenti accessi effettuati verso l'esterno. In assenza dell'osservanza di tali disposizioni, l'Ateneo considera responsabile di ogni azione esercitata attraverso utenze con identificativi di classe privata, l'utente registrato corrispondente ai dati identificativi dell'utenza di rete a cui gli identificativi di classe privata sono associati.
3. Sono svolte in maniera esclusiva dal CESIAT i servizi di posta elettronica di Ateneo e di DNS (Domain Name System). Qualsiasi altro servizio (FTP, http, SSH, etc.) offerto da un *host* della Rete di Ateneo appartenente a Strutture diverse dal CESIAT, deve essere espressamente autorizzato dal CESIAT e dovrà essere erogato in accordo alle politiche di sicurezza e alle specifiche tecniche indicate dal CESIAT. L'Ateneo adotta le misure di sicurezza idonee (firewall, etc.) al fine di bloccare gli accessi alla Rete di Ateneo non autorizzati nonchè l'erogazione di servizi non auorizzati.

Art. 11 - Estensione della Rete di Ateneo

1. Il CESIAT assicura la connessione alla Rete di Ateneo di ogni Rete Locale di Struttura pianificando, sulla base delle disposizioni degli organi di governo dell'Ateneo, i collegamenti e le bande trasmissive previste, in base alle esigenze della Struttura e compatibilmente con le risorse disponibili.
2. Nessuna Struttura può attivare connessioni autonome delle proprie Reti Locali alla Rete di Ateneo o con quelle di altre Strutture di Ateneo, se non in accordo a quanto previsto dal comma 1 del presente articolo. Ogni estensione della Rete di Ateneo, sia relativamente agli apparati attivi che agli apparati passivi, deve essere preventivamente autorizzata dal CESIAT e in ogni caso conforme agli standard tecnologici e di sicurezza da esso adottati.
3. Analoga regolamentazione è da intendersi estesa a tutte le connessioni di reti locali di Strutture connesse alla Rete di Ateneo con Internet Service Provider (ISP) pubblici o privati.
4. Fermo restando quanto stabilito dall'Art. 10 del presente regolamento, in presenza di risorse di personale di adeguata competenza tecnica, parte della gestione della Rete di Ateneo, relativamente alla sottorete corrispondente alle singole Strutture, può essere delegata alle Strutture stesse, fatto salvo l'obbligo di concordare con il CESIAT le politiche di sicurezza adottate, e di verificare con il CESIAT che le soluzioni adottate non compromettano il corretto funzionamento della Rete di Ateneo. Nei casi di funzioni decentralizzate affidate ad una Struttura, il Direttore di tale Struttura nomina un referente tecnico, comunicandone il nominativo con atto formale al CESIAT.
5. L'Ateneo non è in nessuna misura responsabile di attività svolte su Internet attraverso accessi che vengono effettuati autonomamente mediante l'uso di Internet Service Provider (ISP) pubblici o privati. Se una Struttura attiva autonomamente un'accesso ad Internet attraverso ISP pubblici o privati, non essendo le utenze che si avvalgono di tali accessi assimilabili a fruitori della Rete di Ateneo, ma di una rete logicamente diversa, esclusiva responsabilità in ordine alle misure di sicurezza da adottare e agli obblighi di prevenire eventuali abusi connessi ai comportamenti degli utenti su Internet, spettano al Direttore di tale Struttura (Preside, nel caso di una Facoltà).
6. La connessione tra Enti esterni e la Rete di Ateneo dovrà essere valutata caso per caso dagli Organi Accademici sia in relazione alle finalità istituzionali dell'Ente sia alle sue affiliazioni a livello nazionale. In ordine agli obblighi e alle responsabilità dell'Ente e del suo Direttore, valgono le prescrizioni previste dal presente regolamento per le Strutture di Ateneo, tra cui la nomina di un referente tecnico con atto

formale e conseguente notifica al CESIAT. La concessione e il mantenimento della connessione alla rete di Ateneo potranno essere condizionati dalla messa in atto, da parte dell'Ente, di specifiche soluzioni tecniche individuate dal CESIAT allo scopo di garantire livelli di sicurezza adeguati agli standard da esso adottati.

Art. 12 – Panorama Normativo di Riferimento

Le disposizioni contenute nel presente regolamento si collocano nel vasto quadro normativo che regola aspetti penali e civili legati all'utilizzo di tecnologie informatiche. In particolare:

- Legge del 23 Dicembre 1993, n. 547 (reati informatici). Essa amplia le precedenti disposizioni in materia e integra al Codice Penale l'art. 635-bis sul danneggiamento dei sistemi informatici e telematici, l'art. 615-quinquies sulla diffusione di virus e malware, l'art. 392 sulla violenza sulle cose (a tal proposito la legge 547 del 1993 precisa le situazioni dove le aggressioni riguardano beni informatici) ed infine l'art. 420 sul reato di attentato ad impianti di pubblica utilità. La legge 547 del 1993 aggiunge inoltre al Codice Penale l'art 640-ter per punire chiunque cerchi di ottenere un arricchimento interferendo abusivamente nell'elaborazione dei dati. Riguardo le forme di intrusione nella sfera privata altrui si incriminano l'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), la detenzione e diffusione abusiva di codici d'accesso (art. 615-quater c.p.) la rivelazione del contenuto di documenti segreti (art. 621 c.p.) includendo i documenti protetti contenuti su supporti informatici. Circa le aggressioni alle comunicazioni informatiche viene ampliato il concetto di corrispondenza contenuto nel quarto comma dell'art. 616 c.p. che ingloba anche la corrispondenza informatica e telematica e punisce l'intercettazione e l'interruzione di comunicazioni informatiche (art. 617-quater c.p.) e l'installazione di apparecchiature atte ad intercettare o impedire comunicazioni informatiche (art. 617-quinquies), qualora tali condotte non siano esplicitamente autorizzate.
- Art. 40 cpv c.p. Relativamente alla responsabilità dell'autore del comportamento illecito, l'ordinamento penale italiano prevede la categoria dei cosiddetti ***reati omissivi impropri*** che si concretizzano nella violazione di un generico obbligo giuridico di impedire determinati eventi dannosi. Per giurisprudenza e dottrina unanimi, tra le fonti di tale obbligo rientra la posizione di controllo connaturata ad un rapporto di lavoro subordinato. Tale obbligo si applica pertanto anche al caso delle attività illecite svolte attraverso l'uso di sistemi informatici.
- Art. 2043, 2049, 2050 del c.c. Responsabilità civile generica (ex art. 2043) dell'autore di fatto doloso o colposo che cagiona ad altri un danno ingiusto, responsabilità civile oggettiva (ex art. 2049) in relazione ai comportamenti illeciti dei dipendenti, responsabilità civile (ex art. 2050) originatasi nell'esercizio di *attività pericolose.*
- Decreto Legislativo N. 196 del 2003 (protezione dei dati personali, requisiti idonei di sicurezza dei sistemi informatici). Misure di sicurezza da adottare per garantire idonea protezione, disponibilità e affidabilità dei dati trattati. Diritti dei cittadini in ordine alla tutela, correttezza e riservatezza dei propri dati personali.
- Decreto del 16 agosto 2005, emanato dal Ministro dell'interno di concerto con il Ministro delle comunicazioni e con il Ministro per l'innovazione tecnologica, in attuazione a quanto previsto dall'art. 7, comma 4, della legge 31 luglio 2005, n. 155 (legge anti-terrorismo). Il Decreto stabilisce una serie di misure che hanno obbligo di adottare tutti i titolari o gestori di un esercizio pubblico o di un circolo privato di qualsiasi specie nel quale sono poste a disposizione del pubblico, dei clienti o dei soci, apparecchi terminali utilizzabili per le comunicazioni, anche telematiche.
- Decreto Legislativo N. 82 del 7 marzo 2005 aggiornato con le modifiche introdotte dal Decreto Legislativo del 4 aprile 2006 recante disposizioni integrative e correttive (codice dell'amministrazione digitale). Utilizzo delle tecnologie informatiche nelle Pubbliche Amministrazioni.
- Decreto Legislativo N. 518 del 29 Dicembre 1992 e Decreto Legislativo N. 205 del 15 Marzo 1996 (tutela dei diritti sul software).
- Decreto Legislativo N. 169 del 6 Maggio 1999 (tutela del *costitutore* di database).