UNIVERSITA' DEGLI STUDI DI CASSINO

REGOLAMENTO DI ACCESSO ALLA RETE DI ATENEO

Acceptable User Policy

Articolo 1 - Oggetto e ambito di applicazione

L'Università degli Studi di Cassino, consapevole delle potenzialità offerte dagli strumenti informatici e telematici, promuove l'utilizzazione della Rete Informatica e Telematica dell'Università, in seguito indicata con Rete di Ateneo, quale strumento utile, compatibilmente con le proprie strutture e risorse, a perseguire le proprie finalità nel quadro dell'attività istituzionale svolta dall'Università stessa. Rientrano, in particolare, nelle attività istituzionali l'attività di ricerca, la didattica e l'amministrazione.

Il presente Regolamento stabilisce le condizioni e le modalità vincolanti per l'accesso e l'utilizzazione della Rete di Ateneo e dei servizi di rete, L'uso delle risorse e dei servizi della Rete di Ateneo è subordinato al rispetto da parte degli utenti del presente Regolamento, oltre che delle norme civili, penali e amministrative applicabili.

Costituiscono parte integrante del presente Regolamento le norme che regolano la Rete GARR nel loro ambito di applicazione (Allegato A).

Articolo 2 - Definizioni

Ai fini del presente Regolamento, si intendono adottate le definizioni seguenti:

- Rete di Ateneo: l'insieme delle infrastrutture fisiche e logiche e dei servizi che consente la comunicazione e la trasmissione di dati e fonia all'interno e tra le diverse sedi dell'Ateneo nonché tra l'Ateneo e la rete telefonica esterna ed Internet; per quest'ultima, l'accesso avviene, di norma, attraverso la Rete GARR.
- nodo di rete: ogni computer, terminale, stampante, periferica, telefono, fax o dispositivo connessi alla rete di Ateneo;
- utente interno: qualsiasi persona o struttura autorizzata che acceda alla Rete di Ateneo;
- utente esterno: qualsiasi persona o struttura, non autorizzata dal CASI, che acceda ai servizi in rete dell'Università;
- GARR: Gruppo Armonizzazione Reti per la Ricerca;
- CASI: Centro di Ateneo per i Servizi Informatici, struttura responsabile della gestione amministrativa e tecnica della rete di Ateneo, del dominio di secondo livello "unicas.it" e relativi sottodomini e dello spazio di indirizzamento pubblico IP 193.205.60.0/22;
- Referente informatico di struttura: responsabile dell'accesso alla rete di Ateneo relativamente e limitatamente ai nodi collegati in rete di competenza di una data struttura; presa utente: il punto di connessione fonia/dati, al quale può essere collegato un nodo di rete.

Articolo 3 - Facoltà d'accesso alla Rete di Ateneo

Hanno facoltà di accedere alla rete di Ateneo, secondo le modalità di seguito definite e limitatamente al periodo in cui intercorre il rapporto con l'Università:

a. il personale docente afferente all'Università degli Studi di Cassino, nonché i loro collaboratori purché strutturati, i docenti a contratto, i dottorandi, i titolari di borse post-dottorato, i titolari di borse, assegni o contratti di ricerca, i collaboratori alla ricerca;
b. il personale tecnico-amministrativo, compreso il personale a tempo determinato ed i titolari di contratti di collaborazione;
c. i componenti degli organi dell'Università benché non dipendenti dell'Università;
d. gli studenti regolarmente iscritti all'Università o a corsi e seminari;
e. i partecipanti ed i relatori di convegni/seminari gestiti o organizzati dall'Università anche in compartecipazione con altri enti;
f. i collaboratori e i ricercatori esterni impegnati in attività da svolgersi all'interno dell'Università;
g. i consulenti ed i dipendenti/collaboratori di società fornitrici i quali abbiano necessità di accedere alla Rete di Ateneo per lo svolgimento delle attività a cui sono stati preposti.

Potrà essere autorizzato dal CASI l'accesso a singoli utenti o strutture o Enti che non rientrino nelle categorie sopraelencate solo a seguito di motivata richiesta presentata per iscritto dalla struttura di Ateneo interessata. Rientra in tale casistica l'accesso alla Rete d'Ateneo consentito al personale di Enti pubblici o privati in virtù di accordi di Convenzione o di Contratti di ricerca e similari stipulati con strutture d'Ateneo, limitatamente al personale impegnato nelle attività previste in tali accordi e distaccato presso l'Ateneo.

L'accesso alla Rete di Ateneo dovrà comunque ed in qualsiasi caso essere conforme alle regole stabilite dall'Accettable Use Policy (AUP) del GARR che costituisce parte integrante del presente regolamento (Allegato A).

Il CASI o il Referente informatico di struttura, per quanto di propria competenza, può vietare temporaneamente – anche attraverso azioni coercitive sulla infrastruttura di rete - l'accesso alla Rete da parte di nodi di rete, categorie di utenti o singoli utenti, al fine di preservare il buon funzionamento della Rete nel suo complesso.

Articolo 4 - Modalità di accesso alla Rete di Ateneo

L'accesso alla Rete di Ateneo ed ai servizi di rete è regolato in modo da consentire agli utenti la fruizione dei servizi e delle applicazioni informatiche erogate dalle varie strutture nonché, nei casi previsti, l'accesso alla rete Internet tramite il collegamento attivato tramite il GARR.

L'accesso alla rete e l'utilizzo delle risorse avviene conformemente ai dispositivi di legge attualmente in vigore e, in particolare, ma non esclusivamente, gli utenti devono essere a conoscenza ed osservare le sottocitate norme:

- D. Lgs. n. 196/2003 del 30 giugno 2003 "Codice in materia di protezione dei dati personali",
- "Netiquette guidelines", documento noto come "RFC 1855"
- GARR Acceptable Use Policy (AUP)
- D.P.R. 10 novembre 1997, n. 513 (Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59);
- Legge 22 Aprile 1941 in materia di disposizioni sul diritto di autore, con l'aggiornamento del comma 1/b aggiunto dall'Art. 1 D.Lgs. 29/12/1992, n. 518 (Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore);
- Decreto Legge n. 518 del 29/12/1992: Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore;
- Legge n. 547 del 23/12/1993: Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica;

- Legge n. 675 del 31/12/1996: Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (testo coordinato con le modifiche introdotte dai D.L. 9/5/1997 n.123, 28/7/1997 n.255, 8/5/1998 n.135, 13/5/1998 n.171, 6/11/1998 n.389, 26/2/1999 n.51, 11/5/1999 n.135, 30/7/1999 n.281 e 30/7/1999 n.282);
- D.P.R. n. 318 del 28/7/1999: Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675;
- Decreto del Ministro dell'Interno del 16/8/2005: Misure di preventiva acquisizione di dati anagrafici dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili.

Tutta la predetta normativa è disponibile per la consultazione nella sezione "Documentazione" del sito: http://www.casi.unicas.it .

Articolo 5 – Nodi di rete e identificazione degli utenti.

I nodi di rete vengono classificati come segue:

a. nodo ad utilizzo individuale: apparecchiatura collegata alla rete di ateneo di norma utilizzata da una sola persona appartenente ad una delle categorie di cui all'art. 3 punti a,b,c,f,g; ad esempio PC, notebook, telefono (VoIP o tradizionale), stampante di rete ad uso singolo, etc.;
b. nodo ad utilizzo collettivo: apparecchiatura collegata alla rete di ateneo di norma utilizzata da più persone appartenenti alle categorie di cui all'art. 3 punti a,b,c,f,g; ad esempio stampanti di rete e altre apparecchiature condivise, PC condivisi, etc.;
c. switch, hub, router, access-point, bridge wireless o altro apparato attivo per la distribuzione di rete di gestione diretta CASI;
d. switch, hub, router, access-point, bridge wireless o altro apparato attivo per la distribuzione di rete installato e gestito da una particolare struttura dell'Ateneo non direttamente riferibile al CASI;
e. elaboratore server o altra attrezzatura di servizio di diretta gestione CASI;
f. elaboratore server o altra attrezzatura di servizio installato e gestito da una particolare struttura dell'Ateneo non direttamente riferibile al CASI;
g. nodo ad utilizzo individuale o collettivo non controllato: apparecchiatura collegata alla rete di Ateneo di norma utilizzata da più persone appartenenti alle categorie di cui all'art. 3 punti d, e; ad esempio, PC/chioschi, notebook di proprietà degli studenti o dei partecipanti ad un convegno, etc.

Al fine di ottemperare alle normative di cui all'art. 4, tutti gli utilizzatori di apparecchiature in grado di connettersi alla rete Internet sono tenuti ad identificarsi presso il CASI secondo le modalità operative stabilite sul sito http://www.casi.unicas.it . Gli utenti che invece accedono soltanto ai servizi della rete interna di Ateneo (come, ad esempio, gli utilizzatori dei chioschi) non incorrono in tali obblighi.

Articolo 6 – Modalità di interconnessione dei nodi di rete

In generale i nodi di rete vengono collegati alla Rete di Ateneo attraverso l'utilizzo delle prese utente o mediante collegamenti wireless. Nel primo caso dovrà essere posta ogni attenzione affinché i collegamenti avvengano senza comportare danni alla infrastruttura di rete ed alla presa utente ponendo particolare attenzione ad utilizzare materiali e procedure adeguati.

Il collegamento di apparecchiature alla rete di Ateneo, con riferimento alla classificazione riportata all'art. 5, è subordinato al rispetto delle seguenti norme:

a. i nodi ad utilizzo individuale potranno essere collegati alle prese utente solo dopo che l'utilizzatore si è identificato ed ha comunicato al CASI la locazione e la numerazione della presa utente, ottenendone la necessaria autorizzazione;
b. i nodi ad utilizzo collettivo potranno essere collegati alle prese utente solo dopo che il referente informatico della struttura interessata ha comunicato al CASI la locazione e la numerazione della presa utente, ottenendone la necessaria autorizzazione, nonché si è assunto la responsabilità di identificare gli utilizzatori ed i relativi periodi di utilizzo dell'apparecchiatura;
c. gli apparati attivi di diretta gestione CASI vengono identificati e registrati a cura del CASI;
d. gli apparati attivi acquisiti ed installati da strutture diverse dal CASI potranno essere collegati alla rete di Ateneo solo previa autorizzazione del CASI; la configurazione di tali apparati dovrà essere eseguita da personale qualificato concordemente alle indicazioni fornite dal CASI; se tali apparati consentono la gestione (remota e/o locale), la struttura interessata dovrà comunicare al CASI le credenziali per l'accesso agli apparati in modalità "amministratore"; tali apparati potranno essere utilizzati unicamente per distribuire connettività ad utilizzatori che rientrino esclusivamente nelle categorie a,b,c,f,g di cui all'art. 3 e l'identità di tali utilizzatori dovrà essere comunicata al CASI a cura della struttura interessata;
e. gli elaboratori server di diretta gestione CASI vengono identificati e registrati a cura del CASI;
f. gli elaboratori server acquisiti e gestiti da strutture diverse dal CASI potranno essere collegati alla rete di Ateneo solo previa autorizzazione del CASI che potrà essere rilasciata soltanto dopo che la struttura interessata ha comunicato al CASI:
    a. gli estremi identificativi dell'hardware e del software da installare;
    b. il numero ed il tipo (indirizzo di tipo pubblico o privato) dei collegamenti di rete necessari;
    c. le procedure che verranno adottate per mantenere in sicurezza l'elaboratore, con particolare riferimento alla protezione dagli attacchi informatici e all'aggiornamento del sistema operativo e delle applicazioni installate;
    d. la natura dei servizi erogati e dei possibili utilizzatori;
    e. la banda richiesta su ogni interfaccia di rete;
g. i nodi ad utilizzo individuale o collettivo non controllato (es. chioschi) vengono di norma installati e gestiti dal CASI; eventuali richieste di acquisizione ed installazione di tali tipologie di nodi a cura di altre strutture dovranno venir esaminate ed autorizzate singolarmente dal CASI.

Articolo 7 – Responsabilità

La responsabilità della efficienza e della funzionalità della rete è condivisa dal CASI, in quanto gestore e manutentore dell'infrastruttura, e dalle singole strutture o dai singoli utilizzatori in quanto fruitori della rete medesima.

In particolare, la responsabilità dei dati presenti sugli elaboratori e trasmessi sulla rete interna e sulla rete Internet sono da attribuirsi, con riferimento alle lettere della classificazione operata all'art. 5:

a. all'utilizzatore del nodo;
b. al referente informatico della struttura;
c. al CASI;
d. al referente informatico della struttura;
e. al CASI;

f. al referente informatico della struttura e ai gestori dell'elaboratore se appositamente designati ed esplicitamente consenzienti;
g. alla struttura che provvede alla gestione del nodo.

Al fine di ottenere l'autorizzazione all'uso delle risorse di Rete d'Ateneo, l'utente dovrà esplicitamente dichiarare, nella richiesta di accesso:

- di acconsentire al trattamento dei suoi dati personali da parte dell'Ateneo in conformità alle norme legislative e regolamentari vigenti e applicabili;
- di impegnarsi ad osservare il presente Regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono per il tramite della Rete di Ateneo.

Gli utilizzatori ed i gestori delle apparecchiature collegate in rete sono – all'atto stesso di utilizzare una risorsa o gestire i servizi erogati da elaboratori server – consapevoli che l'utilizzo improprio o per scopi diversi da quelli istituzionali delle apparecchiature informatiche può comportare conseguenze sia sul piano della mera funzionalità della rete di Ateneo e delle altre apparecchiature ad essa collegate, sia sul piano penale ed amministrativo.

In particolare, gli utenti della rete di Ateneo sono soggetti a tutte le responsabilità dettate dalla normativa vigente ed applicabile con specifico ma non esclusivo riferimento a quanto segue:

a. l'accesso alle risorse di elaborazione ad uso individuale (punto a. art. 6) è personale e non può essere condiviso o ceduto;
b. la responsabilità del contenuto dei materiali conservati nella memoria degli elaboratori e diffusi attraverso la rete è degli utenti che li producono e diffondono;
c. gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi a cui hanno accesso;
d. le credenziali (nome utente, password, smartcard, etc.) per l'accesso ai sistemi ed alle risorse della Rete di Ateneo devono essere conservati con ogni cura onde evitare che terzi ne vengano in possesso e non devono essere comunicati ad alcuno; l'utente è consapevole che le responsabilità derivanti dall'abuso di credenziali altrui vengono condivise con il legittimo proprietario nel caso quest'ultimo avesse omesso una pronta segnalazione secondo le modalità definite all'art. 10;
e. gli utenti sono obbligati a segnalare immediatamente, secondo le modalità di cui all'art. 9, ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza informatica relativa a dati/procedure di propria pertinenza ma anche di dati/procedure non di propria pertinenza nel momento in cui se ne viene a conoscenza;
f. gli utenti sono tenuti a mantenersi costantemente informati ed aggiornati sulle procedure e sulle modalità di utilizzo della rete di Ateneo, consultando periodicamente le pertinenti informazioni pubblicate sul sito http://www.casi.unicas.it.

Articolo 8 – Centro di Ateneo per i Servizi Informatici (CASI)

L'Università degli Studi di Cassino, al fine di rendere disponibili le risorse tecnologiche necessarie allo svolgimento delle attività istituzionali relative alla ricerca, alla didattica ed alla amministrazione, ha affidato al Centro di Ateneo per i Servizi Informatici (CASI) la realizzazione, gestione e manutenzione (operativa ed evolutiva) della infrastruttura di rete fonia/dati (cablata e wireless) nonché dei servizi e delle applicazioni ad essa connesse.

Pertanto, il CASI assicura in modo esclusivo la gestione, il monitoraggio, l'aggiornamento e l'ampliamento della Rete d'Ateneo (cablaggio e parte attiva) sia sotto l'aspetto fisico che logico, curandone i relativi progetti, fino alla presa utente compresa.

Il CASI, nell'espletamento delle proprie attività di gestione e monitoraggio della rete di Ateneo, potrà raccogliere dati relativi alle attività di rete dei singoli nodi; tali dati saranno soggetti al

trattamento in conformità alla vigente normativa applicabile, verranno utilizzati esclusivamente per le attività istituzionali del CASI e potranno essere comunicate alle autorità giudiziarie a fronte di formale richiesta.

La raccolta di tali dati – effettuata esclusivamente per gli scopi di cui al punto precedente – avverrà comunque per il periodo di tempo strettamente necessario e non su base continuativa se non in forma aggregata e quindi non riconducibile al singolo nodo.

Il CASI ha la facoltà di revocare temporaneamente l'autorizzazione di accesso alla rete di Ateneo o limitare la fruizione di servizi ad uno o più nodi, a seguito di:

a. violazioni del presente Regolamento o della normativa vigente applicabile;
b. generazione di traffico e servizi dannosi o potenzialmente dannosi per il regolare funzionamento della rete di Ateneo nel suo complesso;
c. esigenze di manutenzione ordinaria o straordinaria della rete di Ateneo.

Nel caso a. l'interdizione dovrà essere documentata ed il CASI ha facoltà di trasmettere tale documentazione agli organi competenti dell'Ateneo.

Nel caso b. e se l'evento assume carattere di continuità, il CASI provvede a documentare il provvedimento e trasmetterlo al responsabile del nodo.

Nel caso c. e nel caso si tratti di manutenzione ordinaria, il CASI provvede a comunicare, con congruo anticipo mediante avviso sul sito web http://www.casi.unicas.it, il periodo di interruzione ed i nodi interessati dalla manutenzione, mentre nel caso si tratti di manutenzione straordinaria e questa si protrae per oltre 60 minuti, il CASI provvede a comunicare, con congruo anticipo, la durata dell'interruzione al Referente informatico della struttura o al Responsabile della struttura interessata.

Articolo 9 - Referenti informatici di struttura

I Referenti informatici di struttura rappresentano l'interfaccia amministrativa e tecnica dell'utenza verso il CASI. Il Referente informatico viene nominato dal Responsabile di ogni struttura e, in mancanza di tale nomina, è identificato con il Responsabile della struttura medesima (Facoltà, Dipartimenti, Centri di Servizio, Amministrazione Centrale, Scuole di Specializzazione, etc.);

E' opportuno che ogni struttura d'Ateneo che abbia la responsabilità amministrativa di uno o più nodi di cui all'art. 5 individui, oltre al Referente informatico di cui sopra, anche un sostituto. Un Referente informatico e/o il suo sostituto può essere condiviso fra più strutture, tenendo conto della disposizione logistica delle sedi e della opportunità di tale scelta.

Il Responsabile della struttura dovrà comunicare il nominativo ed i riferimenti telefonici e di posta elettronica del Referente informatico e dell'eventuale sostituto al CASI. Il Referente informatico, a sua volta, riceverà una comunicazione di conferma dal CASI con la quale verrà stabilita anche la data a partire dalla quale sarà considerato nel pieno delle sue funzioni.

Il Responsabile della struttura comunica al CASI anche eventuali cambiamenti dei nominativi dei Referenti informatici, i quali dovranno a loro volta essere esplicitamente confermati dal CASI con le modalità di cui al comma precedente.

I Referenti informatici di struttura sono responsabili dal punto di vista tecnico, all'interno delle singole strutture dell'Ateneo, dei nodi secondo le competenze stabilite all'art. 7. con obbligo di riferirsi al CASI, con le modalità di cui all'art. 10, per ogni violazione o sospetto di violazione di sicurezza informatica e/o del presente Regolamento.

I Referenti informatici di struttura debbono operare secondo le direttive e le procedure stabilite dal CASI con apposite linee guida pubblicate sul sito http://www.casi.unicas.it.

Articolo 10 – Accesso ai servizi online di segnalazione guasti, anomalie, smarrimento o sottrazione di credenziali.

Al fine di armonizzare e strutturare la gestione dei guasti di infrastrutture di rete attive e passive, nonché di nodi di rete di propria competenza, il CASI ha istituito un servizio di richiesta interventi nonché di segnalazione guasti o anomalie (Helpdesk) accessibile attraverso il sito http://www.online.unicas.it a seguito dell'identificazione successiva all'inserimento delle credenziali di utente.

Tali credenziali, per coloro che non ne fossero in possesso, possono essere richieste con le modalità riportate sul medesimo sito.

Per le segnalazioni urgenti relative alla perdita o sottrazione (anche presunta) della proprie credenziali per l'accesso ai servizi online, il CASI istituisce il numero telefonico 0776.2994949 dotato di segreteria telefonica che, in mancanza di un operatore, registra la segnalazione dell'utente. L'utente che si serve del predetto numero telefonico ha l'obbligo di circostanziare l'evento segnalato e comunicare i propri riferimenti senza i quali la segnalazione stessa verrà archiviata.

Articolo 11 - Tutela della riservatezza e controllo delle attività presenti nella rete di Ateneo.

L'Università tutela il diritto alla riservatezza relativo alle comunicazioni supportate dalla Rete di Ateneo e ai dati personali presenti nella rete stessa, in conformità alle norme legislative e regolamentari vigenti e applicabili.

Gli organi competenti dell'Ateneo possono accedere ai dati personali presenti nella rete di Ateneo, nelle circostanze previste dalle norme legislative e regolamentari vigenti e applicabili.

Il CASI mantiene, per i principali flussi di dati, un registro dei collegamenti e delle attività (log) che verrà custodito con ogni cura e riservatezza per gli usi e gli scopi consentiti dalla legge e dai regolamenti dell'Ateneo; tali registri verranno mantenuti almeno per il periodo minimo indicato dalle norme applicabili e, in particolare, quello indicato dal D.Lgs. n. 196/2003 del 30 giugno 2003.

Con la promulgazione del presente Regolamento, il CASI è autorizzato ad utilizzare sistemi di monitoraggio della rete in grado di verificarne la rispondenza a quanto previsto dal presente Regolamento nel rispetto della normativa vigente.

Articolo 12 - Modalità di utilizzazione della rete di Ateneo

La rete di Ateneo può essere utilizzata esclusivamente per gli scopi autorizzati dal presente Regolamento, ossia come supporto alla ricerca, alla didattica, all'amministrazione, e alle altre attività istituzionali dell'Università, nonché come strumento utile alla comunità dell'Ateneo.

E' vietato utilizzare la rete di Ateneo per scopi incompatibili con quelli stabiliti nel presente Regolamento e in violazione della vigente normativa.

In particolare, a titolo esemplificativo e non esaustivo, è vietato:

1. accedere alla Rete 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;
2. usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi; il CASI ed il Referente informatico si riservano la facoltà di impedire in qualsiasi momento l'accesso alla Rete di Ateneo da parte di utenti anonimi o non sufficientemente identificati o identificabili;
3. violare gli obblighi in materia di copyright, licenze d'uso di software;

4. svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, distraggano risorse (persone, capacità, elaboratori), danneggino o restringano l'utilizzabilità o le prestazioni della Rete di Ateneo; è altresì vietato impedire, tentare di impedire o interferire in qualsiasi forma con la fruizione dei servizi offerti tramite la Rete di Ateneo agli altri Utenti e manomettere in qualsiasi modo le apparecchiature e le strutture informatiche ed elettroniche;
5. violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete d'Ateneo e dei quali non si è destinatari specifici;
6. compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
7. distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare, accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri Utenti o di terzi; usare, intercettare o tentare di intercettare, 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;
8. 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 e pedo-pornografiche;
9. utilizzare la Rete Dati di Ateneo e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale, tranne nei casi specificatamente autorizzati dal Rettore;
10. trasferire materiale in violazione delle norme sulla proprietà intellettuale, mediante programmi di tipo "Peer to Peer" o con altri strumenti;
11. installare modem configurati in call-back;
12. accedere ai locali e ai box riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi senza l'autorizzazione del CASI;
13. cablare o collegare apparecchiature alle prese di rete senza l'autorizzazione del CASI; tale autorizzazione va richiesta tramite il servizio di Helpdesk di cui all'art. 10.

Deroghe ai punti 12 e 13 potranno essere valutate nei singoli casi e comunque dovranno essere formalizzate tramite apposito disciplinare (Articolo 6).

Articolo 13 – Ulteriori disposizioni

Le soluzioni informatiche relative a:

- erogazione di servizi su elaboratori server non direttamente gestiti dal CASI;
- utilizzo dei nomi a dominio;
- connessione alla rete di Ateneo di elaboratori con indirizzo IP pubblico;

sono soggette ad esplicita autorizzazione del CASI, da richiedere tramite il servizio di Helpdesk di cui all'art. 10.

Le modalità operative per l'attivazione di tali soluzioni sono esposte sul sito istituzionale del CASI: http://www.casi.unicas.it .

Articolo 14 - Variazione del Regolamento della Rete di Ateneo

Il presente Regolamento è suscettibile di modifiche e/o integrazioni. Tali modifiche e/o integrazioni, proposte dal Presidente del CASI, sono sottoposte all'approvazione degli organi di governo dell'Ateneo (Senato Accademico e Consiglio di Amministrazione).

Tutti gli utenti interni dell'Ateneo vengono informati delle modifiche via e-mail. Il nuovo regolamento entra in vigore senza che vi sia l'obbligo di richiedere nuovamente l'accettazione da parte dell'utente.

Articolo 15 - Violazioni

L'Università adotta ogni misura necessaria per prevenire, reprimere e sanzionare le violazioni al presente Regolamento allo scopo di mantenere in efficienza la Rete di Ateneo ed impedire infrazioni alle norme ed alle leggi applicabili che regolano la materia.

Ricorrendo le condizioni ed al fine di ripristinare la funzionalità della rete, le condizioni di sicurezza dei dati, il rispetto delle norme previste nel presente Regolamento, il CASI può, senza bisogno di preavviso:

- disattivare le credenziali di accesso ai servizi;
- disconnettere un nodo di rete;
- inibire la funzionalità di un nodo di rete, totalmente o parzialmente.

Fatte salve le ulteriori conseguenze di natura penale, civile, amministrativa e disciplinare della violazione compiuta, il CASI ha facoltà di informare gli organi competenti dell'Ateneo a fronte di comportamenti in violazione del presente Regolamento o qualora vi sia il fondato sospetto che ciò sia avvenuto.

Il ripristino dei nodi disattivati, delle funzionalità e delle credenziali utente potrà avvenire soltanto quando il CASI ha verificato la rimozione delle cause della violazione e, se quest'ultima ha avuto carattere di gravità dal punto di vista penale, amministrativo, disciplinare, della sicurezza dei dati e della funzionalità di rete, il ripristino potrà avvenire solo a seguito di esplicito e formale assenso della Direzione Amministrativa o degli organi di governo competenti.

ALLEGATO A

Acceptable Use Policy della rete GARR

(versione del 24.11.2000)

Disponibile all'indirizzo: http://www.garr.it/docs/garr-aup-00.shtml

1. La Rete Italiana dell'Università e della Ricerca Scientifica, denominata comunemente "la Rete GARR", si fonda su progetti di collaborazione scientifica ed accademica tra le Università, le Scuole e gli Enti di Ricerca pubblici italiani. Di conseguenza il servizio di Rete GARR è destinato principalmente alla comunità che afferisce al Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR). Esiste tuttavia la possibilità di estensione del servizio stesso anche ad altre realtà, quali quelle afferenti ad altri Ministeri che abbiano una Convenzione specifica con il Consortium GARR, oppure realtà che svolgono attività di ricerca in Italia, specialmente, ma non esclusivamente, in caso di organismi "no-profit" impegnati in collaborazioni con la comunità afferente al MIUR. L'utilizzo della Rete è comunque soggetto al rispetto delle Acceptable Use Policy (AUP) da parte di tutti gli utenti GARR.
2. Il "Servizio di Rete GARR", definito brevemente in seguito come "Rete GARR", è costituito dall'insieme dei servizi di collegamento telematico, dei servizi di gestione della rete, dei servizi applicativi e di tutti quelli strumenti di interoperabilità (operati direttamente o per conto del Consortium GARR) che permettono ai soggetti autorizzati ad accedere alla Rete di comunicare tra di loro (Rete GARR nazionale).

   Costituiscono parte integrante della Rete GARR anche i collegamenti e servizi telematici che permettono la interconnessione tra la Rete GARR nazionale e le altre reti.
3. Sulla rete GARR non sono ammesse le seguenti attività:
   - fornire a soggetti non autorizzati all'accesso alla Rete GARR il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing, di hosting e simili, nonchè permettere il transito di dati e/o informazioni sulla Rete GARR tra due soggetti entrambi non autorizzati all'accesso sulla Rete GARR (third party routing);
   - utilizzare servizi o risorse di Rete, collegare apparecchiature o servizi o software alla Rete, diffondere virus, hoaxes o altri programmi in un modo che danneggi, molesti o perturbi le attività di altre persone, utenti o i servizi disponibili sulla Rete GARR e su quelle ad essa collegate;
   - creare o trasmettere (se non per scopi di ricerca o comunque propriamente in modo controllato e legale) qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;
   - trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;
   - danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password), chiavi crittografiche riservate e ogni altro "dato personale" come definito dalle leggi sulla protezione della privacy;

- svolgere sulla Rete GARR ogni altra attività vietata dalla Legge dello Stato, dalla normativa Internazionale, nonchè dai regolamenti e dalle consuetudini ("Netiquette") di utilizzo delle reti e dei servizi di Rete acceduti.

4. La responsabilità del contenuto dei materiali prodotti e diffusi attraverso la Rete è delle persone che li producono e diffondono. Nel caso di persone che non hanno raggiunto la maggiore età, la responsabilità può coinvolgere anche le persone che la legge indica come tutori dell'attività dei minori.
5. I soggetti autorizzati (S.A.) all'accesso alla Rete GARR, definiti nel documento "Regole di accesso alla Rete GARR", possono utilizzare la Rete per tutte le proprie attività istituzionali. Si intendono come attività istituzionali tutte quelle inerenti allo svolgimento dei compiti previsti dallo statuto di un soggetto autorizzato, comprese le attività all'interno di convenzioni o accordi approvati dai rispettivi organi competenti, purchè l'utilizzo sia a fini istituzionali. Rientrano in particolare nelle attività istituzionali, la attività di ricerca, la didattica, le funzioni amministrative dei soggetti e tra i soggetti autorizzati all'accesso e le attività di ricerca per conto terzi, con esclusione di tutti i casi esplicitamente non ammessi dal presente documento.

   Altri soggetti, autorizzati ad un accesso temporaneo alla Rete (S.A.T.) potranno svolgere solo l'insieme delle attività indicate nell'autorizzazione.

   Il giudizio finale sulla ammissibilità di una attività sulla Rete GARR resta prerogativa degli Organismi Direttivi del Consortium GARR.
6. Tutti gli utenti a cui vengono forniti accessi alla Rete GARR devono essere riconosciuti ed identificabili. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati. Di norma gli utenti devono essere dipendenti del soggetto autorizzato, anche temporaneamente, all'accesso alla Rete GARR.

   Per quanto riguarda i soggetti autorizzati all'accesso alla Rete GARR (S.A.) gli utenti possono essere anche persone temporaneamente autorizzate da questi in virtù di un rapporto di lavoro a fini istituzionali. Sono utenti ammessi gli studenti regolarmente iscritti ad un corso presso un soggetto autorizzato con accesso alla Rete GARR.
7. E' responsabilità dei soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR di adottare tutte le azioni ragionevoli per assicurare la conformità delle proprie norme con quelle qui esposte e per assicurare che non avvengano utilizzi non ammessi della Rete GARR. Ogni soggetto con accesso alla Rete GARR deve inoltre portare a conoscenza dei propri utenti (con i mezzi che riterrà opportuni) le norme contenute in questo documento.
8. I soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR accettano esplicitamente che i loro nominativi (nome dell'Ente, Ragione Sociale o equivalente) vengano inseriti in un annuario elettronico mantenuto a cura degli Organismi Direttivi del Consortium GARR.
9. In caso di accertata inosservanza di queste norme di utilizzo della Rete, gli Organismi Direttivi del Consortium GARR prenderanno le opportune misure, necessarie al ripristino del corretto funzionamento della Rete, compresa la sospensione temporanea o definitiva dell'accesso alla Rete GARR stessa.
10. L'accesso alla Rete GARR è condizionato all'accettazione integrale delle norme contenute in questo documento.