



AREA INFORMATICA & TELEMATICA

REGOLAMENTO DI ACCESSO AI SERVIZI DI RETE

Nome : Area I&T - Regolamento di Accesso ai Servizi di Rete	File : REGOLAMENTO SERVIZI RETE UNICAL V3 0.doc	Data : 5 febbraio 2008
Versione : V 3.0	Stato: OPERATIVO	



SOMMARIO

PREMESSA	3
ART. 1 - OGGETTO E AMBITO DI APPLICAZIONE.....	3
ART. 2 – SOGGETTI	4
ART. 3 - AMMINISTRATORE DI SISTEMA.....	4
ART. 4 – REFERENTE TECNICO.....	4
ART. 5 - DIRITTO DI ACCESSO	5
ART. 6 - DIRETTIVE GENERALI DI ACCESSO AI SERVIZI DI RETE.....	5
ART. 7 - NORME OPERATIVE PER L'ACCESSO AI SERVIZI DI RETE DELL' ATENEO.....	6
ART. 9 – NORME COMPORTAMENTALI PER GLI UTENTI.....	8
ART. 10 – NORME COMPORTAMENTALI PER GLI AMMINISTRATORI DI SERVER.....	8
ART. 11 - ACCEPTABLE USE POLICY DELLA RETE GARR	9
ART. 12 – SANZIONI.....	11



PREMESSA

L'Università degli studi della Calabria dispone di una moderna e veloce infrastruttura di rete che garantisce la connettività a numerosi dipartimenti e centri sparsi lungo l'intera struttura "a ponte". Studenti, docenti, ricercatori e impiegati utilizzano quotidianamente questa risorsa per motivi di studio, ricerca, lavoro.

La rete dati dell'Università della Calabria dispone di un collegamento a banda larga sul Pop della Rete Nazionale GARR (Gruppo Armonizzazione Reti della Ricerca ovvero il consorzio che connette tra loro gli enti della Ricerca Scientifica Italiana). Tale collegamento non è una risorsa illimitata e per questo motivo può rappresentare un vero e proprio collo di bottiglia qualora non venisse disciplinato l'uso della risorsa "rete" da parte degli utenti. Inoltre, l'entrata in vigore del D.L. 7/03/2005, n.82, "Codice dell'Amministrazione Digitale", sancisce il diritto per i cittadini e le imprese a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali (ART.3) e, in particolare, l'ART. 51 sottolinea la necessità che i documenti informatici debbano essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta. E' facile intuire quindi, che negli anni a seguire ci sarà un costante aumento del numero dei servizi che l'Università della Calabria dovrà erogare garantendo elevati livelli di qualità e di sicurezza. A tal riguardo è necessario che l'utenza rispetti le seguenti norme che rappresentano le linee guida per un buon uso delle risorse informatiche, nello spirito dell'RFC 1855 (Request for Comment 1855 - "Netiquette Guidelines" (www.nic.it/NA/modul.html#g11)) e delle direttive emanate dal GARR.

ART. 1 - OGGETTO E AMBITO DI APPLICAZIONE

Oggetto del Regolamento è l'armonizzazione dei servizi di rete erogati dall'Ateneo, sia ad uso interno che esterno, in ogni sua struttura e funzione, comprendendo le componenti hardware, software, procedurali e organizzative.

Il Regolamento è da applicarsi alla circolazione sulla rete GARR-UNICAL di tutte le tipologie di dati, nelle modalità operative descritte nel seguito.



ART. 2 – SOGGETTI

Si definiscono, per gli scopi del presente regolamento, i seguenti soggetti:

Utente: soggetto con diritto di accesso ai servizi di rete.

Utenti strutturati: docenti e personale tecnico-amministrativo.

Utenti non strutturati: collaboratori esterni, dottorandi, assegnisti, ecc...

Studenti: soggetti regolarmente iscritti ad un corso di laurea o di diploma dell'università degli studi della Calabria o provenienti da altri Atenei a seguito di scambi nell'ambito di programmi nazionali ed internazionali.

Amministratore di sistema: un utente strutturato che gestisce il sistema operativo dell'elaboratore che eroga un servizio di rete e, se non diversamente specificato, anche il servizio stesso.

Referente Tecnico: un utente che si occupa della connessione in rete degli elaboratori appartenenti ad una singola struttura, della gestione degli indirizzi IP e della manutenzione di una o più sottoreti nell'ambito di una sottorete assegnata ad una o più strutture.

AI&T: Area Informatica & Telematica

ART. 3 - AMMINISTRATORE DI SISTEMA

Un Amministratore di sistema è nominato dal Responsabile di struttura di appartenenza del server e deve possedere le necessarie competenze tecniche.

Può coincidere con il Referente Tecnico e ha il compito di mantenere funzionanti, sicuri ed efficienti il server e i servizi di rete, secondo le modalità stabilite dal presente Regolamento, collaborando con l'Amministratore di rete e con il Referente tecnico per ridurre al minimo i rischi di incidente informatico. Comunica al Referente Tecnico, al Responsabile di struttura e all'AI&T ogni evento di rischio informatico.

ART. 4 – REFERENTE TECNICO

Il referente Tecnico è nominato dal responsabile di struttura e deve possedere le necessarie competenze tecniche. Ha il compito di mantenere funzionante, sicura ed efficiente la rete di trasmissione dati della struttura, ivi compresi i dispositivi di rete eventualmente presenti e di gestire gli indirizzi IP della sottorete o delle sottoreti assegnate e gli account del dominio di appartenenza. Deve inoltre collaborare con gli amministratori di sistema a ridurre al minimo i rischi di incidente informatico e di malfunzionamento.



ART. 5 - DIRITTO DI ACCESSO

Hanno diritto di accesso ai servizi di rete erogati dall'Ateneo il personale docente e non docente, gli studenti, i collaboratori temporanei o altri soggetti esterni con rapporti di collaborazione e di ricerca con l'Ateneo, secondo le modalità descritte nel presente Regolamento.

Le strutture che non dispongano al proprio interno di risorse tecniche sufficienti, possono comunque utilizzare i servizi di supporto ed help-desk forniti dall'Area IT, in base alle risorse professionali disponibili e con le modalità che saranno comunicate di volta in volta attraverso il Portale d'Ateneo.

ART. 6 - DIRETTIVE GENERALI DI ACCESSO AI SERVIZI DI RETE

Le modalità di accesso ai servizi variano a seconda delle classi di utenti e di servizi ma richiedono sempre l'assegnazione di password personali e segrete di accesso. L'autorizzazione di accesso viene rilasciata dal referente tecnico o dal Responsabile di struttura.

L'accesso ai servizi di rete, sia Internet che Intranet è consentito esclusivamente per fini istituzionali.

Sono consentite solo le attività che non siano in contrasto con il presente Regolamento e con le norme legislative vigenti, non arrechino danno ad altri utenti o all'Ateneo stesso e siano conformi al documento “**Acceptable Use Policy**” del GARR.

Tra le attività proibite si fa particolare riferimento a:

1. trasgressione della privacy di altri utenti o dell'integrità di dati personali;
2. compromissione dell'integrità dei sistemi o dei servizi;
3. consumo di risorse in misura tale da compromettere l'efficienza di altri servizi di rete;
4. compimento di atti di criminalità informatica e a tutte quelle riportate nell'Art.10.

Come stabilito nella Nota Rettorale n° 4815 del 12/03/2003, caso in cui siano rilevate condizioni di utilizzo dei servizi che violino una o più di tali regole l'Area Informatica & Telematica (AI&T) può sospendere temporaneamente l'accesso ai servizi, informando tempestivamente il Referente Tecnico della sottorete interessata, l'Utente stesso e, nel caso di comportamenti non consentiti o non conformi al presente Regolamento e alle Norme di Legge, il Rettore e/o gli Organi di Governo dell'Ateneo.



ART. 7 - NORME OPERATIVE PER L'ACCESSO AI SERVIZI DI RETE DELL'ATENEO

1. Al fine di limitare al minimo i disservizi sul backbone d'Ateneo è necessario comunicare e concordare con i tecnici dell'Area Informatica & Telematica qualsiasi intervento strutturale si intenda affrontare sullo stesso;
2. E' di fondamentale importanza ai fini legali, poter identificare univocamente l'utilizzatore di un determinato indirizzo IP.
3. Il lancio di un nuovo servizio di rete da parte di un amministratore di sistema dovrà essere comunicato ai tecnici dell'AIT i quali si faranno carico dell'adeguamento delle politiche di sicurezza sul backbone.
4. La presenza di Access Point Wireless, collegamenti XDSL, modem e di qualsiasi altro accesso alternativo che possa rappresentare un pericolo per la sicurezza della LAN d'ateneo all'interno delle varie strutture, va tempestivamente comunicata ed il loro utilizzo concordato con l'Area IT secondo quanto previsto al successivo punto 6..
5. E' vietata l'installazione di Access Point Wireless all'esterno delle strutture: l'erogazione di servizi di connettività outdoor è di esclusiva competenza dell'AIT
6. L'installazione di Access Point Wireless all'interno delle strutture deve essere autorizzata dall'AIT ed, in ogni caso, è necessario attenersi alle seguenti condizioni:
 - a. Non deve essere irradiata alcuna potenza all'esterno delle strutture
 - b. La configurazione dei canali radio non può essere impostata in modalità automatica
 - c. Il canale radio da utilizzare dovrà essere obbligatoriamente quello assegnato dall'AIT
 - d. L'installazione dovrà essere tale da garantire i seguenti requisiti minimi di sicurezza:
 - i. Canale Crittografato
 - ii. Access Point Protetto
 - iii. Verifica dei MAC Address dei client
 - iv. Gestione Account in sicurezza
7. Tutti gli Access Point Wireless non autorizzati dall'AIT dovranno essere rimossi
8. I Firewall dipartimentali dovranno prevedere un canale di accesso al fine di garantire agli amministratori di rete la possibilità di effettuare l'attività di monitoraggio.
9. I Firewall personali potranno essere installati sui client a patto che non vengano filtrati gli IP degli amministratori di rete.
10. E' vietato l'utilizzo di strumenti per il controllo remoto della postazione di lavoro o di un server se non è garantito nessun livello di criptazione sulla connessione punto-punto.
11. E' vietato l'uso dei software Peer To Peer se non per fini di ricerca o didattici. In tal caso è necessario comunicare la necessità all'Area Informatica & Telematica tramite lettera di assunzione di responsabilità firmata dal richiedente.
12. Le singole strutture possono fornire servizi internet/intranet qualora possano garantire i requisiti di sicurezza descritti nel presente Regolamento.
13. Si sollecita fortemente di settare i client ftp in modalità passiva. Saranno abilitate sessioni ftp attive, dietro richiesta, solo verso quei server che non gestiscano procedure alternative.



14. L'Area Informatica & Telematica, in collaborazione con gli amministratori dei vari

dipartimenti, disciplina e regola l'utilizzo dei seguenti protocolli:

- a. http
- b. ftp
- c. telnet
- d. ssh
- e. vpn
- f. smtp
- g. pop3
- h. pop3s
- i. dns

15. L'implementazione di un protocollo non compreso nell'elenco potrà essere attivata previo confronto con gli amministratori delle sottoreti interessate e valutazione delle implicazioni sul piano della sicurezza

Art. 8 – Divieti Specifici e Norme di Legge

1. E' proibito l'uso dei Sistemi in Rete in violazione di norme del Codice Civile o Penale.
2. Si richiamano tutte le norme di legge e gli obblighi in materia di copyright e licenze d'uso dei software.
3. E' vietato compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software
4. Gli utenti non possono violare o tentare di violare i sistemi di sicurezza informatici e inoltre non possono intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete d'Ateneo, che non siano loro diretti.
5. E' vietato un utilizzo della risorsa rete che impedisca, interferisca, o causi in ogni modo danno alle attività degli altri utenti. E' quindi vietato qualsiasi tentativo finalizzato ad occupare in maniera esaustiva una risorsa ed è vietato propagare le cosiddette "Catene di S. Antonio" o gli "Hoax" (falsi allarmi di virus pericolosi) e generare "spam" (messaggi pubblicitari non richiesti) tramite posta elettronica.
6. Gli Utenti non possono utilizzare i Sistemi in Rete allo scopo di molestare, minacciare o inviare messaggi non graditi.
7. Gli utenti non possono in alcun modo mascherare o falsificare la propria identità.
8. Gli Utenti non devono né distribuire e né lanciare virus, worm, trojan o altri programmi simili.
9. Gli Utenti non possono, a meno di specifiche autorizzazioni, rimuovere o modificare alcuna apparecchiatura appartenente alla Rete dati d'Ateneo.



10. Nessuna organizzazione e nessun utente esterno all'Ateneo può utilizzare senza una specifica autorizzazione, i Sistemi in Rete eccetto quelli di pubblico dominio come il servizio di consultazione Bibliotecario, la Rubrica telefonica, il server web, ... etc. Inoltre gli Utenti non possono, deliberatamente e in modo non autorizzato, modificare o tentare di modificare dati contenuti nei Sistemi in Rete.
11. Ciascun Utente è responsabile della sicurezza dei codici e delle password assegnate. Codici e password sono normalmente assegnati a singoli utenti e, di conseguenza, non devono essere condivisi con altre persone senza autorizzazione da parte dell'Amministratore del Sistema. Gli Utenti sono responsabili per ogni attività connessa all'utilizzo dei codici e delle password loro assegnate.

ART. 9 – NORME COMPORTAMENTALI PER GLI UTENTI

1. E' consigliata un'installazione ottimizzata del Sistema Operativo ovvero priva di servizi non necessari.
2. E' prescritta la scelta di password che rispettino i seguenti criteri (in ottemperanza al D.L.196 del 30 giugno 2003 sulla privacy (Allegato B)):
 - lunghezza minima 8 caratteri;
 - non banali ma contenenti lettere, numeri, simboli e segni di interpunzione;
 - scadenza semestrale e, possibilmente, rinnovabile direttamente dall'utente;
3. E' necessario sincronizzare il timer con il server ntp UNICAL ntp.unical.it
4. E' necessario effettuare periodicamente (possibilmente quotidianamente) gli aggiornamenti del Sistema Operativo del proprio PC i quali aiutano a ridurre il numero delle vulnerabilità che possono essere sfruttate da virus, trojan o da eventuali malintenzionati.
5. E' necessario installare sul proprio PC l'antivirus d'Ateneo. E' tuttavia consentito l'utilizzo di altri antivirus di provata qualità che garantiscano comunque un aggiornamento automatico tempestivo. L'Area Informatica & Telematica pubblicherà un elenco aggiornato di antivirus consigliati.
6. Si raccomanda di non aprire mai posta proveniente da sconosciuti e contenente allegati sospetti (.tiff, .exe e ...)
7. Si consiglia sempre di navigare su siti sicuri e affidabili
8. Qualora si riscontri la presenza di un virus o un worm sul proprio PC procedere immediatamente col distacco della connessione di rete per poi richiedere al proprio referente tecnico di procedere con le operazioni di bonifica: aggiornamento del Sistema Operativo, ripulitura con sistema Antivirus o con tool per la rimozione di worm e trojan specifici reperibili presso i siti dei maggiori produttori di antivirus.

ART. 10 – NORME COMPORTAMENTALI PER GLI AMMINISTRATORI DI SERVER

Gli elaboratori con funzioni di server internet devono essere abilitati dagli amministratori di rete dell'AIT, ad essere raggiungibili sia dall'esterno che dall'interno della LAN mediante abilitazioni sui Firewall. Al fine di non compromettere la sicurezza della rete, è opportuno che siano rispettate le seguenti condizioni:



1. Installazione sicura e ottimizzata del sistema operativo.
1. Aggiornamento periodico del sistema operativo e del software applicativo.
2. Disabilitazione dei servizi non necessari.
3. Accesso locale al sistema riservato solo all' Amministratore e all'incaricato del trattamento dei dati (D.L. 196/2003) e da remoto, in modalità cifrata (ad esempio tramite il protocollo SSH).
4. Scelta di password che rispettino i seguenti criteri (in ottemperanza al D.L.196 del 30 giugno 2003 sulla privacy (Allegato B)):
 - lunghezza minima 8 caratteri;
 - non banali ma contenti lettere, numeri, simboli e segni di interpunzione;
 - scadenza semestrale e rinnovabile;
5. Sincronizzazione del timer con il server ntp UNICAL ntp.unical.it
6. Configurazione dei meccanismi di logging, in particolare per gli accessi e i servizi.
7. Configurazione e pianificazione delle procedure di backup.
8. Custodia sicura delle informazioni di logging e di backup nel rispetto delle vigenti norme sulla privacy.
9. Accesso riservato e protetto alle informazioni di logging ed, eventualmente, di auditing;
10. Protezione da accessi non autorizzati.
11. Protezione contro virus informatici mediante adozione di un adeguato sistema antivirus.
12. Protezione fisica da accessi incontrollati.
13. Adozione di adeguati meccanismi di ripristino del sistema e di rilevazione delle intrusioni.

ART. 11 - ACCEPTABLE USE POLICY DELLA RETE GARR

1. La Rete Italiana dell'Università e della Ricerca Scientifica, denominata comunemente "la rete del GARR", si fonda su progetti di collaborazione scientifica ed accademica tra le Università e gli Enti di Ricerca pubblici italiani. Di conseguenza il servizio di rete GARR è destinato principalmente alla comunità che afferisce al Ministero dell'Università e della Ricerca Scientifica e Tecnologica (MURST). Esiste tuttavia la possibilità di estensione del servizio stesso anche ad altre 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 MURST. 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 quegli strumenti di interoperabilità (operati direttamente o per conto del 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, nonché 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) e chiavi crittografiche riservate;
 - svolgere sulla rete GARR ogni altra attività vietata dalla Legge dello Stato, dalla normativa Internazionale, nonché 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.
5. I soggetti autorizzati (S.A.) all'accesso alla rete GARR, definiti nel documento "Regole approvate dalla CRCS", 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, purché 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 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 autorizzati 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 GARR.
9. In caso di accertata inosservanza di queste norme di utilizzo della rete, gli Organismi Direttivi 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.

ART. 12 – SANZIONI

Qualora siano riscontrate attività non conformi al presente regolamento, l'AIT invierà, al Responsabile di Struttura ed all'Amministratore di sistema, formale richiesta di adeguamento con termine perentorio di due giorni lavorativi. Trascorso tale termine, se la Struttura non avrà provveduto agli adeguamenti necessari, l'AIT sospenderà l'erogazione dei servizi di rete. L'AIT potrà ripristinare i servizi di rete alla Struttura interessata solo dopo aver accertato la rimozione delle cause di difformità.