UNIVERSITA' DEGLI STUDI DI PARMA

REGOLAMENTO DI ACCESSO AI SERVIZI DI RETE

SOMMARIO

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 del Polo

GARR-PARMA di
tutte le tipologie di dati, nelle modalità operative descritte nelle "**Norme di attuazione**
del regolamento di accesso ai servizi di rete dell'Ateneo", di seguito indicate con
Norme.

La validità del Regolamento si estende pertanto anche alle reti locali afferenti agli altri
membri del Polo GARR-PARMA, interconnesse con le reti locali di Ateneo, che nell'in-
sieme costituiscono la rete del Polo GARR-PARMA.

Ogni interconnessione esterna alla rete del Polo GARR-PARMA deve essere autorizzata
e conforme al presente Regolamento.

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 e dottorandi.

Studenti: soggetti regolarmente iscritti ad un corso di laurea o di diploma dell'Ateneo
di Parma 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.

Amministratore di rete: un utente strutturato che si occupa della connessione in rete
degli elaboratori appartenenti ad una singola struttura.

Referente di dominio: la persona che si occupa della distribuzione e della gestione degli

indirizzi IP nell'ambito di un dominio assegnato ad una o più strutture

Responsabile di struttura: il Direttore della struttura che fornisce servizi Internet e
Intranet.

CCE: Centro di Calcolo Elettronico.

Art. 3 - Organi di riferimento

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

GARR, Gruppo Armonizzazione delle Reti di Ricerca (www.garr.it), in particolare
l'Organismo Tecnico Scientifico (OTS), di nomina ministeriale, e il Nucleo Tecnico GARR-
CRUI. Il GARR è autorevole, tramite il Comitato GARR-PARMA, per le modalità di
accesso a Internet.

Comitato GARR-PARMA, costituito da rappresentanti dell'Università di Parma, dei
Gruppi INFN e INFM di Parma e degli organi del CNR operanti a Parma, è autorevole
per l'accesso alla rete GARR nazionale e per la gestione delle classi di indirizzi IP
assegnate all'Ateneo dai competenti organi internazionali.

Centro di Calcolo Elettronico, di seguito chiamato CCE, che ha funzioni di sviluppo,
pianificazione, aggiornamento, gestione, controllo e manutenzione dell'infrastruttura
di rete dell'Ateneo.

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

Art. 4 - Gruppo di Sicurezza Informatica

Viene costituito il Gruppo di Sicurezza Informatica, indicato

successivamente con GSI,
con compiti di controllo e di coordinamento operativo dell'attuazione tecnica del
Regolamento secondo le modalità descritte nelle Norme. E' l'organo principale di
riferimento tecnico per la sicurezza dei servizi di rete.

Il GSI, sulla base dell'evoluzione tecnologica nel settore o di variazioni apportate al
Regolamento o comunque ogniqualvolta riscontri evidenti e documentabili esigenze
tecniche o funzionali, può modificare le Norme, purché rimangano conformi al Regola-
mento.

Il GSI è coordinato dal Rettore o da un suo delegato e può avvalersi della collaborazione
del CCE e del Comitato GARR PARMA. Del Gruppo, di nomina rettorale, possono far
parte docenti, tecnici ed esperti di comprovata competenza nell'erogazione di servizi

informatici e telematici.

Il GSI non ha compiti di implementazione dei servizi di rete.

Il GSI informa il Rettore e i Responsabili di struttura in caso di incidente informatico, di
intrusione non autorizzata e di inosservanza del Regolamento.

Art. 5 - Amministratore di sistema

Un Amministratore di sistema:

è nominato a tempo indeterminato dal Responsabile di struttura di appartenenza del
server e deve possedere le necessarie competenze tecniche;

può coincidere con l'Amministratore di Rete e con il Referente di dominio;

ha il compito di mantenere funzionanti, sicuri ed efficienti il server e i servizi di rete,
secondo le modalità stabilite dalle Norme, collaborando con l'Amministratore di rete e
con il Referente di dominio per ridurre al minimo i rischi di incidente

informatico;

comunica al Referente di dominio, al Responsabile di struttura e al GSI ogni evento di
rischio informatico.

La sua nomina, rinuncia o sostituzione va formalmente comunicata al GSI tramite il
"Modulo di Assunzione di Responsabilità, conformemente a quanto descritto nelle
Norme.

Art. 6 - Amministratore di Rete

L'Amministratore di rete:

è nominato a tempo indeterminato dal Responsabile di struttura e deve possedere le
necessarie competenze tecniche;

può coincidere con l'Amministratore di sistema e con il Referente di dominio;

ha il compito di mantenere funzionante, sicura ed efficiente la rete di trasmissione dati
della struttura, ivi compresi i dispositivi di rete eventualmente presenti.

La sua nomina, rinuncia o sostituzione va formalmente comunicata al GSI tramite il
"Modulo di Assunzione di Responsabilità conformemente a quanto descritto nelle
Norme.

Art. 7 - Referente di Dominio

Il Referente di Dominio:

è nominato a tempo indeterminato dal Responsabile di struttura e non necessariamente
deve possedere competenze informatiche e/o telematiche;

ha il compito di assegnare e gestire i nomi e gli indirizzi di rete per gli utenti della

struttura di afferenza;

può coincidere con l’Amministratore di rete e con l’Amministratore di sistema;

comunica tempestivamente al GSI e al Responsabile di struttura ogni incidente che
pregiudichi la sicurezza e collabora con il GSI per l'attuazione delle contromisure
necessarie;

La sua nomina, rinuncia o sostituzione va formalmente comunicata al GSI tramite il
"Modulo di Assunzione di Responsabilità conformemente a quanto descritto nelle
Norme.

Art. 8 - Responsabile di Struttura

Il Responsabile di Struttura:

è il Direttore della struttura che accede ad un servizio di rete;

delega le funzioni operative a collaboratori di comprovata competenza tecnica di cui agli
Art.5, 6, 7 e predispone tutte le condizioni organizzative, logistiche ed amministrative
affinché questi possano svolgere efficacemente il proprio mandato, ivi compresa la
formazione permanente degli amministratori dei servizi erogati dalla struttura;

deve fornire al GSI tutte le informazioni relative all’organizzazione dei servizi erogati
dalla struttura, in particolare i nominativi di chiunque abbia funzioni di gestione ed
amministrazione dei servizi di rete;

può emanare regolamenti di accesso ai servizi con validità interna alla struttura, purché
conformi con il Regolamento.

Art. 9 - Sito web di Ateneo

Il Servizio Relazioni Pubbliche è il referente per la pubblicazione di pagine sul sito web di Ateneo. Può avvalersi di gruppi di lavoro composti da esperti del settore, nominati dal Rettore per specifici progetti finalizzati alla sperimentazione di soluzioni ed innovazioni tecniche da proporre agli organi accademici.

Art. 10 - 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 nelle Norme.

Le strutture che non dispongano al proprio interno di risorse tecniche sufficienti, possono comunque accedere ai servizi di rete attraverso il CCE.

Art. 11 - 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, così come descritto nelle Norme;

l'autorizzazione di accesso viene rilasciata dal Responsabile di struttura;

l'accesso ai servizi di rete, sia Internet che Intranet, deve essere compatibile con le "Direttive di sicurezza dei servizi di rete emanate dall'Ateneo, ed è consentito esclusivamente per fini istituzionali;

sono consentite solo le attività che non siano in contrasto con il 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.

Art. 12 - Diritto di erogazione di un servizio di rete

Una struttura può erogare servizi di rete compatibilmente con le proprie risorse e
comunque in osservanza del Regolamento.

Art. 13 - Direttive di sicurezza

I principi fondamentali di sicurezza dei servizi di rete erogati dall’Ateneo sono descritti
nel documento "Direttive per la sicurezza dei servizi di rete dell’Ateneo.

Art. 14 - Architettura di sicurezza

L’erogazione dei servizi di rete di Ateneo avviene attraverso un’adeguata architettura
di sicurezza, la cui implementazione è coordinata dal GSI ed è descritta nelle Norme.

Art. 15 - Sanzioni

Il GSI può sospendere temporaneamente l’accesso ai servizi informando il Rettore, nel
caso di comportamenti non consentiti o non conformi al Regolamento e alle Norme.

Art. 16 - Norme transitorie e finali

Il Regolamento viene attuato in via sperimentale per un periodo di 12 mesi dalla sua
emanazione, secondo le modalità contenute nelle Norme. Dopo gli eventuali adeguamenti
viene emanato dal Rettore ed aggiornato, su proposta del GSI,

ogniqualvolta le mutate
esigenze dell'Ateneo o le innovazioni tecnologiche lo impongano, e comunque almeno
ogni due anni, conformemente ai periodici aggiornamenti del DPR 318/99 sulle misure
minime di sicurezza.

L'Ateneo mette a disposizione le risorse per l'attuazione del Regolamento e per la
formazione permanente del personale addetto alla gestione dei servizi di rete, in misura
e secondo modalità deliberate dagli Organi Accademici sulla base delle esigenze e degli
sviluppi tecnologici del settore.

APPENDICE I

Panorama normativo di riferimento

Dlgs.n.518 del 29.12.1992, che riguarda la tutela giuridica del programmi per elaboratore;

Legge n.547 del 23.12.1993,
che modifica il codice penale introducendo i crimini informatici;

Legge n.675 del 31.12.1996,
che disciplina il trattamento dei dati personali;

Legge n.59 del 15.3.97
che introduce l'equivalenza tra documento cartaceo e documento digitale.

Decreto del Presidente della Repubblica 28 luglio 1999 n.318:"Regolamento recante
norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati
personali a norma dell'articolo 15, comma 2, legge 31.12.96 n.675.

Il Regolamento si ispira alle "Linee guida per la definizione di un piano di sicurezza dei
sistemi informativi automatizzati nella Pubblica Amministrazione " dell'AIPA.

Il Regolamento fa proprio i principi contenuti nello Statuto, con particolare riferimento

all’Art.1 "Principi fondamentali ", Art.5 "Diritto e dovere di informazione ", e il decreto
353/22353 del Consiglio di Amministrazione "Regolamento di attuazione delle norme
sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali ".

APPENDICE II

Acceptable Use Policy del GARR

Alla data di emanazione del Regolamento è disponibile una versione preliminare delle
Acceptable Use Policy del GARR. Il documento definitivo sostituirà integralmente le
norme qui riportate.

1. Il "Servizio di rete GARR ", definito brevemente in seguito come "Rete GARR ",
costituito dall’insieme dei servizi di collegamento telematico, dei servizi di gestione
della rete, dei servizi applicativi e di tutti quelli strumenti di interoperabilità che
permettono ai soggetti autorizzati all’accesso di comunicare tra di loro (rete GARR
nazionale).

Fanno parte della rete GARR anche i collegamenti e servizi telematici che permettono
la interconnessione tra la rete GARR nazionale e le altre reti accademiche e della
ricerca, nonché tra la rete GARR nazionale e tutti gli altri servizi di rete da essa
raggiungibili, in particolare la cosiddetta "rete Internet ".

2. I soggetti autorizzati all’accesso alla rete GARR possono utilizzare la rete per tutte le
proprie attività istituzionali, con l’eccezione dei casi in cui il soggetto è autorizzato
all’accesso alla rete GARR solamente per un insieme limitato di attività e/o periodo
temporale. In mancanza di tale esplicita limitazione, si intendono come attività
istituzionali tutte quelle inerenti allo svolgimento dei compiti previsti dallo statuto

di un soggetto ammesso, comprese le attività all'interno di convenzioni o accordi
approvati dai rispettivi organi competenti.

Rientrano in particolare nelle attività istituzionali, la attività di ricerca, la didattica,
le funzioni amministrative e le attività per conto terzi, con esclusione di tutti i casi
esplicitamente non ammessi dal presente documento.

Nota: a titolo di esempio, non è da considerare attività istituzionale la creazione di
un sito Web dedicato a prodotti commerciali di terzi, mentre invece è ammissibile
ospitare un sito Web destinato ad una associazione culturale senza fini di lucro con
cui esista una convenzione.

Il giudizio finale sulla ammissibilità di una attività sulla rete GARR resta prerogativa
dell'OTS-GARR.

L'accesso alla rete GARR è condizionato all'accettazione integrale delle norme
contenute in questo documento.

3. Sulla rete GARR non sono ammesse le seguenti attiv ità:

• fornire a soggetti non ammessi 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;

• permettere il transito di dati e/o informazioni sulla rete GARR tra due soggetti
entrambi non ammessi all'accesso sulla rete GARR (third party routing);

• utilizzare servizi o risorse di rete in un modo che danneggi o molesti altre persone o
che attenti alla dignità umana;

• creare o trasmettere (se non per scopi di ricerca o comunque propriamente in modo

controllato e legale)qualunque immagine, dato o altro materiale offensivo, osceno o
indecente, specialmente se riguardante il sesso, la razza o il credo;

• creare o trasmettere materiale finalizzato allo scopo di arrecare disturbi o produrre
ingiustificate preoccupazioni;

• creare o trasmettere materiale diffamatorio;

• trasmettere materiale che viola i diritti di autore;

• trasmettere materiale commerciale e/o pubblicitario non richiesto;

• sprecare risorse di rete, dei calcolatori connessi o risorse del personale addetto al loro
funzionamento;

• danneggiare, distruggere o cercare di accedere senza autorizzazione a dati di altri
utenti;

• violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di
parole di accesso (password)riservate;

• interferire nel lavoro di altri utenti;

• impedire l'uso della rete GARR ad altri utenti (ad esempio sovraccaricando le linee
di accesso o gli apparati di commutazione);

• accedere alla rete GARR con apparecchiature o software che interferiscono con il
corretto funzionamento della rete stessa o di altre reti ad essa collegate;

• disseminare virus, hoaxes o altri programmi la cui presenza danneggia la rete e/o le
risorse ad essa collegate;

• svolgere sulla rete GARR ogni altra attività vietata dalla Legge dello Stato, dalle
normative vigenti nei Paesi ospitanti i servizi di rete che

vengono acceduti, dalla normativa Internazionale in materia nonché dai regolamenti e dalle consuetudini ("Netiquette ")di utilizzo delle reti e dei servizi di rete acceduti.

4. 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 o assimilabili del soggetto che accede alla rete GARR.

Nota: a titolo di esempio sono utenti ammessi i visiting professors e gli utenti di un laboratorio scientifico. Sono utenti ammessi anche gli studenti regolarmente iscritti ad un corso presso un soggetto (Università, Scuola di Specializzazione, etc.)con accesso alla rete GARR, purché gli studenti accedano alla rete GARR tramite le strutture (sala terminali, postazioni li lavoro, sala corsi, etc.)collocate fisicamente presso il soggetto dove si tengono i corsi.

5. Ogni soggetto con accesso alla rete GARR deve sottoporre ai propri utenti (con i-mezzi che riterrà opportuni)le norme contenute in questo documento.

Nota: Si consiglia inoltre di redigere norme per l’accesso ai servizi di rete a disposizione a livello locale che siano in armonia con le direttive contenute in questo documento, o che rimandino direttamente ad esse.

6. Tutti i soggetti con accesso alla rete GARR si devono impegnare ad adottare e diffondere tecniche e strumenti che consentano il risparmio della banda condivisa (mirror, proxy, compressione, ecc.), nonché il corretto uso delle risorse e dei servizi di rete.

7. La responsabilità del contenuto dei materiali prodotti e diffusi

attraverso la rete
delle persone che li producono e diffondono ed esula dalle responsabilità dei soggetti
ammessi sulla rete GARR e degli amministratori della rete GARR stessa.

8. E ‘responsabilità dei soggetti con accesso alla rete GARR di prendere 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.

E’ inoltre compito di ogni soggetto con accesso alla rete GARR nominare le seguenti
posizioni:

• un Access Point Manager (APM), con responsabilità prevalentemente tecnico opera-
tive definite nel documento "Compiti di un APM ";

• un Access Point Administrator (APA), con responsabilità prevalentemente ammini-
strativo giuridiche definite nel documento "Compiti di un APA ".

Queste persone costituiscono l’interfaccia privilegiata tra il soggetto con accesso alla
rete GARR e gli organismi ed i servizi operativi sulla rete GARR stessa.

I fruitori della rete GARR devono inoltre fornire alla Direzione GARR (o a chi da essa
esplicitamente indicato)la massima collaborazione per rintracciare ed impedire gli
usi non ammessi della rete GARR stessa.

9. I soggetti ammessi all’accesso 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 della Direzione GARR.

10. L’OTS-GARR, qualora individui usi impropri della rete che non siano fatti cessare
dopo opportuna segnalazione ai responsabili dei soggetti con

accesso alla rete GARR
coinvolti, si riserva la facoltà di prendere le opportune misure operative e/o
giuridiche necessarie al ripristino del corretto funzionamento della rete, compresa la
sospensione temporanea o definitiva dell’accesso alla rete GARR stessa, come
indicato in dettaglio nel "Regolamento Operativo della rete GARR ".