Norme Tecniche Attuative della “Normativa dell'Ateneo di Genova per la realizzazione e gestione della rete dati”

Premessa

Le norme tecniche attuative della “Normativa dell'Ateneo di Genova per la realizzazione e gestione della rete dati”, descritte nel presente documento, hanno l’obiettivo di esplicitare per il responsabile di struttura, i referenti ICT e l'utente finale, le procedure per l’attivazione e la gestione dei servizi, le modalità operative per l'erogazione/fruizione di servizi e per lo sviluppo dell'infrastruttura.

Gli obiettivi generali della Normativa di riferimento sono di aumentare l'affidabilità del sistema e l'accessibilità, l'integrità e la riservatezza delle informazioni trattate. L'armonizzazione, attraverso le norme elencate nel presente documento, ha l’obiettivo di ridurre sia i “rischi” informatici sia eventuali anomalie gestionali, ed il fine ultimo di migliorare il quotidiano svolgimento delle attività accademiche, amministrative e il rispetto della normativa vigente.

Le procedure saranno opportunamente e tempestivamente aggiornate a fronte dei contributi ricevuti, di cambiamenti organizzativi o aggiornamenti tecnologici. In caso si richiedano in futuro modifiche significative, le norme attuative saranno sottoposte all’attenzione degli organi accademici competenti. Per le procedure già di uso comune viene riportato il testo o il link alla relativa pagina web. Per facilitare la consultazione, si intende effettuarne la pubblicazione on-line mediante wiki e FAQ.

Il presente documento rispecchia la struttura del documento “Normativa dell'Ateneo di Genova per la realizzazione e gestione della rete dati” (Regolamento-reti.doc) redatto e discusso in precedenza; e’ stata mantenuta la corrispondenza ordinale degli articoli e sono state esplicitate le procedure ed i riferimenti solo dove il Regolamento lasciava ambiguità di interpretazione.

Art. 1 - Definizioni

Eventuali aggiornamenti alle definizioni ed ulteriori dettagli tecnici sono reperibili agli indirizzi internet:

a) GENUAnet : http://www.csita.unige.it/genuanet/
b) GENUAwi-fi : http://GENUAwifi.unige.it/
c) UniGePASS: http://UniGePASS.unige.it/
d) Rete GARR : http://www.garr.it/
e) AUP (Acceptable Use Policy) di GARR: http://www.garr.it/reteGARR/aup.php?idmenu=collegare (Allegato A)

Art. 2 – Gestione del Sistema Integrato di Reti d'Ateneo

Eventuali aggiornamenti alle definizioni ed ulteriori dettagli tecnici sono reperibili agli indirizzi internet:

1) Il Centro Servizi Telematici e Informatici di Ateneo (CSITA): http://www.csita.unige.it/
2) L'accesso preferenziale al supporto tecnico di CSITA avviene attraverso l'help desk: http://www.csita.unige.it/servizi/aiuto/
3) -.
4) -.
5) -.

Art. 3 - Realizzazione delle reti locali delle strutture

1) –
2) a) Le richieste di adeguamento rete saranno presentate a CSITA attraverso il modello (1) allegato.
3) -
4) -

Art. 4 - Interconnessione delle reti locali di struttura al sistema di reti di Ateneo, alla Rete della Ricerca (GARR) e a Internet

1) -
2) -
3) -
4) -
5) La procedura di configurazione è attivata attraverso l'Helpdesk (Rif. Art 2 Comma 2, punto2). La configurazione concordata tra il referente ICT con i tecnici CSITA attraverso telefono, email incontri.
6) La normativa vigente comprende: Il Codice delle Comunicazioni Elettroniche (DL 259 del 01/08/2003), il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) e successive modificazioni, la legge sulla privacy (Legge 12 luglio 2006 n. 228[1]), il Decreto del Ministro dell'interno del 16 agosto 2005 (G.U. N.190 del 17/8/2005) sulle 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, ai sensi dell'articolo 7, comma 4, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio

1 http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana .

2005, n. 155.

Art. 5 - Protocolli supportati

1) La comunicazione preventiva deve avvenire attraverso il modulo per il censimento dei servizi (modello 5 allegato), sezione 'Note'.
2) Il direttore tecnico di CSITA comunica alle strutture interessate le tempistiche di adeguamento che non dovranno comunque superare un anno solare.
3) **Piano indirizzamento IP:**

L'utilizzo di indirizzi IP pubblici della classe 130.251.0.0/16 per le postazioni dei singoli utenti ha evidenziato vulnerabilità informatiche poiché un qualsiasi PC collegato alla rete può potenzialmente essere visibile ed esposto a un attacco proveniente dall'esterno della rete Genuanet. L'utilizzo di indirizzi IP privati consente ai PC di non essere visibili direttamente su internet.

Assegnamento previsto.

- Rete pubblica: 130.251.0.0/16 utilizzata da tutte le strutture solo per le postazioni che danno un servizio censito verso internet. (ed eventuali estensioni di indirizzamento IPV6[2] fornito da GARR)

- Rete privata: 10.186.0.0/16 utilizzata da tutte le strutture per le postazioni aperte al pubblico (biblioteche, laboratori, ecc.), per le postazioni utilizzate solo per la navigazione su Internet attraverso proxy di Ateneo e che non devono accedere alle applicazioni Intranet.

- Rete privata: 10.187.0.0/16[3] utilizzata da tutte le strutture in sostituzione dell'equivalente rete pubblica, per le postazioni accessibili solo al personale, e che devono poter accedere alle applicazioni Intranet.

- Rete privata: 10.188.0.0/19 utilizzata esclusivamente per la rete wireless GENUAwi-fi

Modalità di attuazione.

In una prima fase di implementazione le sottoreti private della classe 10.187.0.0/16 saranno sovrapposte fisicamente alle corrispondenti sottoreti pubbliche per consentire all'utenza il passaggio in modo graduale. Il passaggio coinvolgerà ogni Facoltà/Struttura concordando le modalità e le tempistiche di intervento con i rispettivi responsabili e referenti.
A regime, le sottoreti private dovranno, ove possibile, rimanere separate fisicamente da quelle pubbliche.
Per semplificare la gestione degli accessi su tutti i firewall presenti all'interno della rete di ateneo, le postazioni amministrative dovranno transitare da indirizzi IP pubblici a indirizzi IP privati secondo la seguente regola:

130.251.x.y -> 10.187.x.y

Gli indirizzi privati dovranno essere registrati sui DNS di ateneo (zona unige.local) o di struttura, previa delega.

---

[2] Vedi documento http://ip6.com/it/paper/migr/migr.htm
[3] La suddivisione prevista per la rete 10.187.0.0/16 è la seguente:
La sottorete 10.187.0.0/22, composta da 4 sottoreti di classe C, sarà assegnata all'interno di CSITA.
Le sottoreti di classe C dalla 10.187.4.0/24 alla 10.187.47.0/24 rimangono da assegnare.
La Sottorete 10.187.48.0/20 composta da 16 sottoreti di classe C, sarà assegnata alle strutture
La Sottorete 10.187.64.0/18 composta da 64 sottoreti di classe C, sarà assegnata alle strutture
La Sottorete 10.187.128.0/17 composta da 128 sottoreti di classe C, sarà assegnate alle strutture

Art. 6 - Referenti ICT di Struttura

1) La comunicazione della nomina del referente/i di struttura e del sostituto/i da parte del Responsabile della struttura per le problematiche di rete ed informatiche, avviene attraverso la compilazione del modello 2 allegato. Strutture distribuite sul territorio possono nominare più referenti per le sedi distaccate.
2) I corsi di formazione ed aggiornamento per i referenti, organizzati da CSITA in collaborazione con l'Ufficio preposto alla formazione del personale tecnico-amministrativo dell'Ateneo, saranno pubblicati al sito http://intranet.unige.it/personale/formazione/
3) -.
4) Le comunicazioni ai referenti avvengono attraverso i comuni media email e/o fax. Mezzo preferenziale sarà la posta elettronica firmata con certificati personali.
5) Le comunicazioni da parte dei referenti agli utenti di struttura avvengono attraverso i comuni media email e/o telefono.
6) -.
7) I referenti sono tenuti a mantenere aggiornata la corrispondenza tra indirizzo IP ed utilizzatore, a registrare l'indirizzo sul DNS di Ateneo o di Struttura se esiste, e a curare l'attribuzione degli indirizzi IP.

Art. 7 - Accesso alla rete

1) -.
2) L'Allegato A indicato nella Normativa e' sostituito dall'indirizzo internet definito in questo documento all'Art. 1 comma e.
3) -.
4) A tal fine l'Universita' fornisce le credenziali UniGePASS definite all'Art. 1 comma c, il processo di identificazione si completa attraverso l'Art. 6, comma 7. I dati sono protetti e trattati in accordo con il Documento Programmatico sulla Sicurezza (DPS) dell'Universita' di Genova[4], e gli obblighi previsti dalla corrente normativa sulla privacy.
5) L'utilizzo delle credenziali UniGePASS risponde ai requisiti minimi previsti dalle normative di legge vigenti in materia di identificazione dell'utente;
6) -
7) Come previsto all'Art. 6 comma 7.
8) -
9) Attraverso filtraggio sugli apparati di rete e richieste di supporto tecnico di pronto intervento da parte dei referenti ICT di struttura. CSITA applica dei filtri di base alla frontiera allo scopo di limitare la diffusione di virus e per un razionale utilizzo della connettività messa a disposizione da GARR. Le regole di dettaglio sono definite in accordo con i referenti tecnici delle strutture coinvolte.

Art. 8 - Registrazione e uso di nomi a dominio

1) L'Ateneo di Genova è titolare di un insieme di indirizzi di rete pubblica IPv4 nell'insieme '130.251', CSITA definisce per l'Ateneo il piano di indirizzamento e gestisce il Domain Name Server (DNS) per i domini e sottodomini di unige.it e unige.eu.

[4] http://www.unige.it/privacy/dps.shtml

2) I responsabili delle strutture possono richiedere la registrazione e l'assegnazione di sottodomini, che non siano già in uso, utilizzando i modelli 3 e 4 allegati.
3) La Procedura per la registrazione di domini di III livello avviene attraverso il modello 3.
4) La richiesta di registrazione di un sottodominio di secondo livello (quindi diverso da unige.it e unige.eu) per .it o .eu e l'associazione ad host con indirizzi IP di Ateneo, deve essere effettuata utilizzando il modello 4. La registrazione e' ammissibile solo se il dominio in oggetto sarà utilizzato in accordo con le finalità di utilizzo della rete GARR, per attività di ricerca e didattiche, senza fini di lucro (vedi anche Art. 1 comma e). Il responsabile della struttura richiedente deve produrre all'APA (Access Point Administrator)[5] dell'Ateneo in ambito GARR, il modello 4 adeguatamente compilato, allegando una nota informativa sull'utilizzo del nome a dominio. La richiesta viene inoltrata dall'APA al GARR.

   L'APA valuta la richiesta e, in caso di approvazione, invia il modulo di richiesta dominio al GARR.

   Se il GARR accetta la richiesta, l'APA lo comunica al responsabile della struttura che dovrà inviare la lettera di assunzione di responsabilità al GARR e al Registro del ccTLD.it. Il GARR-NIC procede quindi alla registrazione del nuovo nome a dominio.

   In caso una Struttura abbia necessità di registrare un nome a domino che risulti già occupato nel ccTLD.it e .eu, dopo aver registrato il nome desiderato all'interno del gTLD.info o .museum, può richiedere all'APA l'associazione ad host con indirizzi IP di Ateneo compilando adeguatamente il modello 4bis.

5) L'eventuale rinnovo periodico è a cura del responsabile della struttura che ha richiesto l'attivazione.
6) -.

Art. 9 - Applicazioni e servizi sulla rete

1) Il documento tecnico di riferimento e' : http://tools.ietf.org/html/rfc1855
2) Procedura di registrazione server: al fine di ottimizzare la gestione della rete e garantire la massima funzionalità possibile ai calcolatori ad essa collegati, è necessario che ogni responsabile di struttura segnali a CSITA i server che erogano servizi "intranet e/o internet"(ad esempio sito web e server di posta) attraverso la compilazione del modello 5 allegato, per il censimento dei servizi di rete. Questo consente a CSITA di adottare misure mirate a garantire ai server priorità nel ripristino, di assegnare maggiore banda per le comunicazioni, di differenziare la politica dei blocchi sulle porte usate dal servizio (ad esempio per spedire e ricevere messaggi di posta elettronica). CSITA renderà disponibile ai referenti ICT e ai responsabili di struttura la consultazione di un database di server e servizi noti e, in seguito, consentirà la compilazione on-line del modello 5.

   Per i servizi 'intranet' l'autenticazione deve avvenire attraverso le credenziali 'UniGePASS'. L'implementazione di servizi on line, da parte delle strutture, che facciano uso delle credenziali di accesso UniGePASS, avviene attraverso la richiesta d'uso con il modello 6 allegato.
3) -.

Art. 10 - Responsabilità dell'utente

1) Le normative vigenti di principale rilevanza sono la legge sulla privacy Legge 12 luglio 2006, n. 228; i derivanti requisiti sull'autenticazione vengono forniti attraverso l'autenticazione 'UniGePASS'(http://UniGePASS.unige.it/) le cui principali funzionalità sono riepilogate nell'allegato modello 7.
2) Le norme e gli aggiornamenti sono pubblicati al sito https://www.csita.unige.it/norme/ .Verrà data comunicazione di eventuali aggiornamenti attraverso le procedure previste dall'Ateneo di Genova (lista genuanet@unige.it e, eventualmente postale interna). Le strutture, attraverso il coordinamento dei propri referenti ICT, realizzano gli aggiornamenti necessari all'implementazione delle misure

[5] http://www.garr.it/cgi-bin/dbutils/apalist.pl

tecnologiche e procedurali richieste.

Art. 11 - Accesso alla rete attraverso tecnologia wireless

1). Le reti wireless sono fondate su tecnologie in continua evoluzione che offrono al personale, studenti ed ospiti dell'Ateneo significativi servizi e riduzione dei costi dei cablaggi. I potenziali pericoli per la sicurezza in fase di accesso e di trasmissione rendono indispensabile l'adozione di una policy, che garantisca elevata qualità di servizio e livelli di sicurezza analoghi alla rete cablata di Ateneo. Obiettivo di questa policy è quindi definire regole e responsabilità per la progettazione di reti wireless, per l'installazione e gestione degli access point (AP), per l'allocazione e l'uso delle frequenze, e per le modalità di accesso wireless ai servizi on-line da parte dell'utente. La policy sarà adeguata periodicamente da CSITA sulla base dell'evoluzione della tecnologia e alle modalità di sviluppo e gestione di GENUAnet. La policy si applica a tutte le zone di connettività wireless di GENUAnet, attraverso tutti gli apparati AP wireless che utilizzano gli indirizzi IP dell'Ateneo, ogni edificio e area esterna annessa e ogni sede remota direttamente connessa alla rete di Ateneo. Poiché le reti wireless possono fornire connettività a chiunque raggiunga l'area di propagazione del segnale dell'Access Point, le barriere fisiche non sono sufficienti per prevenire accessi illeciti, pertanto il collegamento a GENUAnet attraverso Access Point non adeguatamente configurati consentirebbe accesso a utenti non identificati e autorizzati e potrebbe compromettere la sicurezza di apparati, archivi e servizi di rete.

2) Accesso utente a GENUAwi-fi. La rete wireless GENUAwi-fi di Ateneo, è utilizzabile dagli utenti che dispongono delle credenziali personali UniGePASS; il processo di autenticazione e accesso è gestito centralmente da CSITA.

L'accesso alla rete GENUAwi-fi avviene tramite un portale (Captive Portal) che, grazie al protocollo https, permette di proteggere il traffico generato dall'utente al momento dell'immissione delle credenziali UniGePASS. A garanzia dell'autenticità del Captive Portal, gli utenti dovranno verificare l'autenticità del certificato digitale presentato dal portale stesso al momento della connessione.

A seconda delle credenziali, all'utente viene attribuito un profilo differenziato (ospite/studente/staff) di autorizzazione all'uso della rete wireless. Al primo accesso è richiesta la sottoscrizione e l'accettazione dell'informativa inserita nel modello 8 allegato.

3) Procedura per autorizzazione presenza AP wireless, non appartenenti a GENUAwi-fi, nelle sedi dell'Università' di Genova.

Il Decreto del 16 agosto 2005 (G.U. N.190 del 17/8/2005) richiede all'Università di consentire l'uso delle reti wireless a dipendenti, studenti e coloro che in modo occasionale possono utilizzare la connessione ad Internet solo previa autenticazione con credenziali personali.

La connessione, attraverso un qualsiasi media trasmissivo di un access point wireless, alla rete GENUAnet costituisce un ampliamento della rete informatica che sottostà al presente regolamento. È pertanto necessario che la struttura interessata all'attivazione o al mantenimento in funzione di un qualsiasi AP wireless, anche se non esplicitamente connesso alla rete GENUAnet, invii preventivamente a CSITA una richiesta sottoscritta dal responsabile, utilizzando il modello 9 allegato, analogamente alla procedura seguita per le reti cablate.

Sono inoltre richieste le seguenti misure minime:

1. Devono essere operative tutte le misure necessarie per l'autenticazione dell'utente con credenziali personali e la memorizzazione degli accessi (log) secondo le modalità di legge.
2. Devono essere attribuiti indirizzi IP privati e deve essere consentita la navigazione solo attraverso proxy.

3. La navigazione su Internet deve essere consentita solo previa accettazione di liberatoria da parte dell'utente per il salvataggio dei log del proxy, specificando che i log, in caso di richiesta, sono a disposizione dell'Autorità' Giudiziaria.
4. Access Point e postazioni wireless devono costituire una rete separata (fisica o virtuale) del comprensorio/campus rispetto alle lan di struttura.
5. Gli Access Point ad accesso libero che non richiedono alcuna forma di autenticazione da parte dell'utente devono essere adeguatamente riconfigurati a cura della struttura o rimossi.
6. Non e' necessario che la comunicazione via etere venga criptata, purché l'utente venga messo a conoscenza dei rischi nel caso di utilizzo di protocolli insicuri attraverso apposita informativa (modello 8).

CSITA effettua periodicamente il monitoraggio proattivo delle reti wireless. Gli AP che causano interferenze e gli AP non autorizzati potranno essere rimossi, previa comunicazione ai responsabili di struttura.

Art. 12 - Accessi alla rete dall'esterno

1) Modalita' di accesso via VPN e WebVPN. Attraverso l'utilizzo del software VPN client tutti gli utenti possono realizzare una connessione sicura da qualsiasi punto della rete internet, verso l'interno della rete universitaria. Questo implica la possibilità di accedere alle risorse informatiche dell'Università' in modo equivalente al trovarsi fisicamente all'interno dell'Ateneo. Tutti gli utenti possono fare richiesta del servizio riportato compilando adeguatamente il modello 10 allegato. Nei casi in cui si rendesse necessario per un utente accedere a risorse web, il cui utilizzo è riservato a studenti e personale dell'Università di Genova, solo dall'interno della rete di Ateneo (per motivi di sicurezza o condizioni contrattuali), è possibile utilizzare l'accesso via WebVPN (http://webvpn.unige.it) attraverso qualunque browser. WebVPN rappresenta la modalità più immediata, ad esempio, per consultare anche da casa periodici elettronici e banche dati messi a disposizione dal Sistema Bibliotecario.
2) L'attivazione autonoma di servizi di accesso remoto da parte di una Struttura deve essere notificato attraverso il modello 5, sezione 'Altri servizi'.

Art. 13 - Violazioni

La Procedura per la gestione degli incidenti di sicurezza è ispirata alle regole della rete GARR e, in particolare, rappresenta il complemento delle norme di gestione incidenti approvate da GARR-OTS (http://www.cert.garr.it/incidenti.php3).
La procedura viene attivata a seguito della rilevazione di un incidente tramite il sistema di monitoraggio di GENUAnet oppure a fronte di una segnalazione di incidente che coinvolga soggetti appartenenti a GENUAnet oppure entità autoritative (ad es. GARR, Polizia Postale etc.).
Le comunicazioni da CSITA verso i soggetti coinvolti vengono inviate tramite posta elettronica dall'indirizzo abuse@unige.it (con firma elettronica). Qualora la gravità del problema sia tale da compromettere il buon funzionamento dei servizi on-line di importanza cruciale per l'Ateneo, CSITA applicherà immediate misure di protezione, limitando l'accesso a Internet, a GENUAnet o alla rete di comprensorio, per il calcolatore che ha originato l'incidente. Nei casi in cui emergessero problematiche particolarmente complesse per le quali non fosse possibile intervenire puntualmente, CSITA si riserva la possibilità di limitare l'utilizzo di specifici protocolli dandone immediata comunicazione ai referenti ICT.

Al fine di ottimizzare la gestione della rete e garantire, in caso di incidenti, la massima funzionalità possibile ai calcolatori ad essa collegati, ogni responsabile di struttura segnala a CSITA i server che erogano servizi "intranet e/o internet"(ad esempio sito web, server di posta etc.) attraverso la compilazione del modulo per il censimento dei servizi di rete (modello 5) e dei suoi aggiornamenti. In mancanza di segnalazione specifica si assume che tutte le macchine rientrino nella categoria dei client e saranno applicati i criteri associati a questa categoria.

La procedura di gestione degli incidenti prevede i seguenti passi:

1). All'incidente e' assegnato un numero univoco

2). Se l'incidente è pericoloso per il funzionamento della rete o di una sua parte, sono presi dei provvedimenti immediati (ad esempio blocco dell'accesso diretto a Internet)

3). CSITA invierà una comunicazione al referente tecnico e, se noto, all'amministratore di sistema dei calcolatori/servizi coinvolti. Qualora la struttura non abbia indicato un referente tecnico, la segnalazione verrà inviata al responsabile della struttura e al delegato CSITA (v. http://www.csita.unige.it/settori/assdelegati.html) . La comunicazione comprende:

a) sintetica descrizione dell'incidente
b) origine della segnalazione (ad esempio GARR-CERT)
c) descrizione delle eventuali azioni già intraprese da CSITA (ad esempio blocco dell'accesso diretto a Internet)
d) richiesta di intervento sulla macchina per la risoluzione del problema entro un tempo commisurato alla gravità dello stesso
e) indicazione delle misure per la limitazione dell'accesso alla rete che potranno essere successivamente adottate da CSITA;

In caso l'incidente sia stato segnalato da terzi, CSITA risponderà anche a coloro che hanno effettuato la segnalazione, inviando una comunicazione con il numero assegnato all'evento e aggiornandoli sulle iniziative intraprese.

4). Qualora i referenti/responsabili locali non intervengano nel tempo richiesto, CSITA provvederà ad applicare i necessari filtri e/o limitazioni di banda, inviandone comunicazione ai referenti/responsabili locali. In caso di incidente segnalato CSITA potrà inviare a coloro che hanno dato notizia dell'incidente la comunicazione di "problema neutralizzato".

5). Dopo che i referenti/responsabili locali avranno comunicato l'avvenuta risoluzione del problema, CSITA, a valle dell'esito positivo di un controllo, provvederà a rimuovere le eventuali limitazioni precedentemente applicate. In caso di incidente segnalato da terzi, CSITA invierà a coloro che hanno segnalato dell'incidente la comunicazione di "problema risolto". In mancanza di risposta, filtri e/o limiti di banda rimangono applicati a tempo indeterminato.

Art. 14 - Norme tecniche attuative

1) Il presente documento, le norme tecniche attuative e i moduli allegati[6] sono pubblicati al sito web https://www.csita.unige.it/norme/ ed hanno effetto immediato. Eventuali aggiornamenti hanno effetto dalla comunicazione di pertinenza, effettuata secondo gli standard procedurali dell'Università di Genova.

[6] http://intranet.unige.it/modulistica/reteinformatica/index.html

Allegati

modello (1)

Al Centro Servizi Informatici e Telematici di Ateneo
Università degli Studi di Genova
Viale Cembrano, 4 – 16148 Genova
Tel. +39 10 353 2690
Fax +39 10 353 6518

Oggetto: **Richiesta Adeguamento Rete Informatica**

Struttura richiedente: .....

Richiesto cofinanziamento 50%: (si/no) .....

Motivazione: (obsolescenza, guasto, adeguamento, ampliamento,…) .....

Descrizione sintetica dei lavori di adeguamento proposti:
.....
.....
.....

Note:
.....
.....

Il responsabile della struttura .....

modello (2)

Al Centro Servizi Informatici e Telematici di Ateneo
Università degli Studi di Genova
Viale Cembrano, 4 – 16148 Genova
Tel. +39 10 353 2690
Fax +39 10 353 6518

C.C. A …..…….. (referente)
C.C. A …..…….. (referente)

Oggetto: Referente/i ICT di Struttura

Il sottoscritto Prof. ……., Direttore del Dipartimento .....

Comunica a CSITA il nominativo del/dei referenti ICT operanti presso la struttura in oggetto.

Per la sede: ….……..…… il Sig./Dott…….…… ed il sostituto Il Sig./dott. .....

Per la sede:…….…… il Sig./Dott…….…….. ed il sostituto Il Sig./dott. .....

Genova,

_____
Il Direttore

(modello 3)

Al Centro Servizi Informatici e Telematici di Ateneo
Università degli Studi di Genova
Viale Cembrano, 4 – 16148 Genova
Tel. +39 10 353 2690
Fax +39 10 353 6518

Oggetto: richiesta di registrazione del dominio di III livello ..... unige.it (1)

Il sottoscritto.....
Direttore/Preside …… del.....
chiede la registrazione del dominio in oggetto, assumendosi le responsabilità che derivano dall'utilizzo e dalla gestione del nome a dominio (2)

Il sottoscritto chiede a C.S.I.T.A. la definizione del dominio sui server DNS di Ateneo e indica come referente per le problematiche di carattere tecnico:

Nome ..... Cognome .....……

e-mail ..... Tel …….....……

Dati da compilare a cura del referente tecnico:

1) indica come record MX (server di posta in entrata) le macchine

(campo da compilare obbligatoriamente)

nome/indirizzo IP …….

nome/indirizzo IP …….

2) indica come postmaster del dominio

(campo da compilare obbligatoriamente)

indirizzo e-mail …….

3) indica, se presenti, come dns primari, le macchine:

nome/indirizzo IP …….

nome/indirizzo IP …….

4) indica, se presente, come server web, la macchina:

nome/indirizzo IP …….

Data..... Firma.....

(1) Il nome e' subordinato a vincoli tecnic i (Caratteri ammessi: dalla "a" alla "z"; dallo "0" al "9"; il segno "-" , ma non a inizio e/o fine nome. Lunghezza del nome: minimo 3, massimo 63) e organizzativi.

(2) norme di utilizzo della rete GARR riportate alla pagina http://www.garr.it/docs/garr-b-aup.shtml

(modello 4)

All'APA (Access Point Administrator) GARR dell'Università degli Studi di Genova c/o CSITA

Oggetto: Richiesta di registrazione dominio di II livello (1)

..... .it

..... .eu

Il sottoscritto.....

Direttore/Preside …… del.....

chiede la registrazione del dominio in oggetto, allegando la nota informativa sull'utilizzo che si intende fare del nome a dominio (2). Il sottoscritto chiede a C.S.I.T.A. la definizione del dominio sui server DNS di Ateneo e indica come referente per le problematiche di carattere tecnico:

Nome ..... Cognome .....……

e-mail ..... Tel …….....……

Dati da compilare a cura del referente tecnico:

1) indica come record MX (server di posta in entrata) le macchine
(campo da compilare obbligatoriamente)

nome/indirizzo IP ……

nome/indirizzo IP ……

2) indica come postmaster del dominio
(campo da compilare obbligatoriamente)

indirizzo e-mail ……

3) indica, se presenti, come dns primari, le macchine:

nome/indirizzo IP ……

nome/indirizzo IP ……

4) indica, se presente, come server web, la macchina:

nome/indirizzo IP ……

Data..... Firma.....

(1)Caratteri ammessi: dalla "a" alla "z"; dallo "0" al "9"; il segno "-" (ma non a inizio e/o fine nome). Lunghezza del nome: minimo 3, massimo 63

(2)norme di utilizzo della rete GARR riportate alla pagina http://www.garr.it/docs/garr-b-aup.shtml

(modello 4bis)

All'APA (Access Point Administrator) GARR dell'Università degli Studi di Genova c/o CSITA

Oggetto: Richiesta di definizione di dominio di II livello sui server DNS

□ **..... .info**

□ **..... .museum**

Il sottoscritto.....

Direttore/Preside …… del.....

comunica la registrazione del dominio in oggetto, allegando la nota informativa sull'utilizzo che si intende fare del nome a dominio (1). Il sottoscritto chiede a C.S.I.T.A. la definizione del dominio sui server DNS di Ateneo e indica come referente per le problematiche di carattere tecnico:

Nome ..... Cognome .....……

e-mail ..... Tel …….....……

Dati da compilare a cura del referente tecnico:

5) indica come record MX (server di posta in entrata) le macchine
(campo da compilare obbligatoriamente)

nome/indirizzo IP …….

nome/indirizzo IP …….

6) indica come postmaster del dominio
(campo da compilare obbligatoriamente)

indirizzo e-mail …….

7) indica, se presenti, come dns primari, le macchine:

nome/indirizzo IP …….

nome/indirizzo IP …….

8) indica, se presente, come server web, la macchina:

nome/indirizzo IP …….

Data..... Firma.....

(1) norme di utilizzo della rete GARR riportate alla pagina http://www.garr.it/docs/garr-b-aup.shtml

(modello 5)

UNIVERSITA'
DI GENOVA

Modulo per il censimento dei servizi di rete

Per ogni server è obbligatoria l'indicazione di almeno un amministratore. è possibile la compilazione di un solo modulo quando lo stesso amministratore gestisce più macchine.

Struttura _____

Responsabile _____

Amministratori[7]:

1. Nome e cognome _____

Tel _____ Cell_____ Email _____

2. Nome e cognome _____

Tel _____ Cell_____ Email _____

Istruzioni per la compilazione:

- Si intende per *server* qualunque host che fornisca servizi via rete o utilizzi servizi di rete con modalità tipica dei server (es. workstation Linux con MTA locale (Sendmail, Postfix etc.) ,che agisce come server SMTP per gli utenti locali). Vanno indicati tutti i server controllati dagli amministratori sopra elencati.

- Nel campo relativo al server indicare il nome DNS o la denominazione corrente.Nel caso di host *multihomed* (con più indirizzi o più schede di rete), devono essere riportati tutti gli indirizzi IP utilizzando una colonna per indirizzo

- Per ogni servizio fornito, nelle colonne relative ai singoli server indicare la rete da cui essi sono accessibili (Internet / GENUAnet[8])

7 Indicare come amministratore una persona in grado di intervenire sulla macchina anche se non dipendente dell'Ateneo

8 Per server che forniscono servizi solo all'interno de GENUAnet si consiglia l'uso di un indirizzamento privato appartenente alla classe 10.186.x.x

	Server 1	Server 2	Server 3	Server 4
Nome:				
Indirizzo IP				

Servizio	**Porta**				
SMTP in uscita					
SMTP in ingresso	25				
SMTP SSL	465				
POP3	110				
POP3 SSL	995				
IMAP4	143				
IMAP4 SSL	993				
HTTP	80				

HTTPS	443				
FTP	21				
Telnet	23				
SSH	22				
NFS	111				
NNTP	119				
X11	6000-6063				
Condivisione di file e stampanti per reti Microsoft o Samba	135,137, 139, 445				
DNS	-----				
PROXY					

Altri servizi	**Porta**				
Note					

Data _____ Il Responsabile di Struttura _____

modello (6)

Al Centro Servizi Informatici e Telematici di Ateneo
Università degli Studi di Genova
Viale Cembrano, 4 – 16148 Genova
Tel. +39 10 353 2690
Fax +39 10 353 6518

Oggetto: Richiesta di utilizzo di UniGePASS per autenticazione utenti

Il sottoscritto ..... in qualità di .....
chiede di poter utilizzare UniGePASS per l'accesso al servizio .....
..... dal server .....

A tal fine dichiara che :

- UniGePASS sarà utilizzato esclusivamente per effettuare l'autenticazione
- le credenziali utente transiteranno su connessioni cifrate (dall'utente e verso il server di autenticazione UniGePASS)
- le credenziali utente non saranno registrate localmente
- sul server ☐ è/☐ sarà installato un certificato X.509 emesso da ☐ COMODO CA[9] / ☐ GARR-CA /☐ UNIGE-CA / ☐ .....
- l'accesso al sistema sarà effettuato dalle sole persone sotto elencate:

○amministratori/sviluppatori del servizio :

nome e cognome ..... matricola .....
mail ..... tel. .....

nome e cognome ..... matricola .....
mail ..... tel. .....

○amministratori del server:

nome e cognome ..... matricola .....

mail ..... tel. .....

nome e cognome ..... matricola .....

mail ..... tel. .....

○incaricati per il trattamento dei dati personali relativi al servizio:

nome e cognome ..... matricola .....

mail ..... tel. .....

nome e cognome ..... matricola .....

mail ..... tel. .....

Genova, ...

Firma del richiedente Firma del responsabile di struttura[10]

9 Opzione raccomandata per server internet e per servizi erogati agli studenti
10 Se diverso dal richiedente

(modello 7)

Le Credenziali UniGePASS
L'Università fornisce a ogni studente e dipendente le credenziali personali (**nome utente** e relativa **password**) UniGePASS per accedere alla maggior parte dei servizi informatici dell'Ateneo. I servizi che accettano le credenziali UniGePASS sono identificati dal logo 'UniGePASS'. Alcuni dei servizi che permettono l'accesso con il nome utente e la password UniGePASS sono ad esempio:

- Servizio di posta elettronica di Ateneo, compresi Webmail, sistema antispam, servizio di liste.
- Servizio di posta elettronica per gli studenti
- Siti di e-learning AulaWeb
- Alcuni portali e siti di facoltà e dipartimenti
- Accesso ai computer in aree e laboratori studenti

Il Personale strutturato
Al personale dell'Ateneo sono comunicate le proprie credenziali personali sui cedolini paga. Le credenziali vengono stampate sui primi tre cedolini ricevuti. E' possibile (raccomandabile) cambiare la propria parola chiave periodicamente.

Gli Studenti
Le credenziali sono comunicate all'immatricolazione. La password UniGePASS **non** corrisponde al codice segreto del badge. Gli studenti iscritti prima dell'anno accademico 2007/08 possono trovarsi in una di queste situazioni:

- il **nome utente** è costituito dal numero di matricola preceduto da una "S" maiuscola;
- per chi ha richiesto la casella prima del 1° agosto 2002 il **nome utente** corrisponde al numero di matricola;
- gli studenti che utilizzavano servizi di posta elettronica di Giurisprudenza o del DISI hanno mantenuto il relativo **nome utente**;

In caso di smarrimento, una nuova password può essere richiesta direttamente allo Sportello dello Studente della propria Facoltà, a seguito di identificazione personale, senza bisogno di essere a conoscenza della precedente. Nel caso non fosse possibile accedere allo Sportello dello Studente, è possibile contattare l'helpdesk all'indirizzo assistenza@unige.it.

I Collaboratori e altri utenti
I responsabili delle strutture possono richiedere l'assegnazione delle credenziali a nuovi utenti contattando il servizio di helpdesk. L'attivazione può essere richiesta congiuntamente alla richiesta di attivazione della casella di posta.

Le Caselle di struttura e altri servizi collettivi
Per particolari esigenze, possono essere attivati servizi che richiedono l'accesso di più persone.
In questo caso, le credenziali UniGePASS fornite funzionano solo per il servizio collettivo richiesto.

La Sicurezza UniGePASS e il cambio Password.

Il regolamento di Ateneo sulla "privacy" prescrive che la password venga cambiata all'assegnazione e successivamente almeno ogni sei mesi, l'operazione puo' essere eseguita al link [11]. I requisiti minimi richiesti dal vigente regolamento sono:

- lunghezza superiore o uguale a 8 caratteri
- usare lettere, numeri e almeno un carattere tra . ; $! @ - > <
- non utilizzare date di nascita, nomi o cognomi propri o di parenti

[11] http://UniGePASS.unige.it/sicurezza.html

- diversa dal numero di matricola e dalla user-id
- custodirla sempre in un luogo sicuro e non accessibile a terzi
- non divulgarla a terzi ne condividerla con altri utenti

In particolare, è opportuno cambiare la password dopo ogni uso delle credenziali UniGePASS in ambienti estranei.

La Riservatezza

Per garantire la riservatezza della password e dei trasferimenti di dati, ovunque possibile è disponibile la modalità SSL/TLS. I certificati digitali necessari sono forniti da CSITA; (http://www.csita.unige.it/servizi/posta/sicurezza.html); questo richiede che, per un funzionamento ottimale, i certificati radice vengano installati sul proprio computer..

(modello 8) Informativa per utente GENUA-wifi

Condizioni e norme di utilizzo dei servizi di GENUA-wifi

1. Oggetto

1.1 Il presente accordo definisce le condizioni generali di gestione del servizio di rete senza fili GENUA-wifi dell'Università di Genova.

1.2 Con il primo utilizzo del servizio, l'utente dichiara di aver attentamente letto ed espressamente accettato tutti i termini e le condizioni di utilizzo del servizio espressamente indicate nel presente accordo.

2. Obblighi dell'utente

2.1 L'utente s'impegna a non consentire l'utilizzo, a qualunque titolo, del servizio a terzi, del cui comportamento in rete si assume comunque, ai sensi del presente accordo, la responsabilità. L'utente si obbliga a non cedere il presente accordo a terzi, a titolo gratuito o oneroso, temporaneamente o definitivamente, senza il consenso espresso dell'Ateneo.

2.2 L'utente si impegna a non utilizzare il servizio per effettuare comunicazioni che arrechino danni o turbative alla rete o a terzi o che violino le leggi e i regolamenti vigenti. In particolare, in via esemplificativa e non esaustiva, l'utente si impegna a non immettere in rete, attraverso il servizio, materiale in violazione della legge sul diritto d'autore, o di altri diritti di proprietà intellettuale o industriale.

2.3 L'utente si impegna a:

3) utilizzare il servizio per i fini istituzionali e personali per cui è stato concesso, in particolare si impegna a non utilizzare il servizio per fini commerciali;
4) non inviare tramite posta elettronica messaggi pubblicitari e/o promozionali o comunicazioni ad altri utenti e/o gruppi di discussione senza che sia stato richiesto ed ottenuto il relativo consenso ovvero senza che tale invio sia stato sollecitato in modo esplicito (spam);
5) non trasferire grosse moli di dati, se non effettivamente necessario;
6) non violare il segreto della corrispondenza personale e il diritto alla riservatezza;
7) non utilizzare reti Ad-Hoc o altri strumenti (ad esempio sniffer) nelle aree di copertura che potrebbero influenzare negativamente le prestazioni della rete oltre che violare il diritto alla privacy degli utenti dell'ateneo;
8) rispettare le norme di buona educazione in uso sulla rete Internet, note come "Netiquette" divenute standard nel documento noto come "RFC 1855";
9) rispettare Acceptable Use Policy (AUP) della Rete Italiana dell'Università e della Ricerca Scientifica, denominata comunemente "la rete del GARR";
10) rispettare le regole e le indicazioni operative che gli verranno date dall'Ateneo;
11) non trasmettere materiale e/o messaggi che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;
12) non immettere in rete informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio o offensivo.

2.4 L'utente garantisce l'utilizzo di programmi a lui legittimamente concessi su licenza o di aver ottenuto l'autorizzazione all'impiego dell'hardware e del software necessari per fruire del servizio.

2.5 L'utente si impegna a non utilizzare PC forniti di scheda wireless occupando il canale radio per scopi diversi da quelli di ricevere il servizio di rete wireless fornito dall'Università.

3. Responsabilità

3.1 L'utente è responsabile di ogni violazione del presente accordo e si impegna a manlevare, sostanzialmente e processualmente, l'Università, ed a tenerla indenne da qualsiasi pretesa anche di terzi a qualsivoglia titolo, comunque avente causa della violazione del presente accordo e/o dalla violazione di leggi o regolamenti o provvedimenti amministrativi.

3.2 L'utente si assume ogni responsabilità ed onere circa il contenuto e le forme delle comunicazioni realizzate tramite il servizio e si impegna a tenere indenne l'Ateneo da ogni pretesa o azione che dovesse essere rivolta all'Università medesima da qualunque soggetto, in conseguenza a tali comunicazioni. Con tale presa di responsabilità, l'utente esonera espressamente l'Ateneo da qualunque responsabilità e onere di accertamento e/o controllo al riguardo.

3.3 L'utente s'impegna a tenere indenne l'Università da tutte le perdite, danni, costi e oneri, ivi comprese le eventuali spese legali, che dovessero essere sostenute dall'Ateneo in conseguenza dell'utilizzo del servizio

messo a disposizione dell'utente.
3.4 Il servizio di rete wifi è fornito mediante l'utilizzo di frequenze in banda condivisa e limitata protezione contro interferenza, dunque l'erogazione del servizio e la sua qualità non sono garantite.
3.5 L'Università non sarà responsabile verso l'utente e/o suoi aventi causa e verso terzi per i danni diretti, indiretti o consequenziali, le perdite e i costi supportati in conseguenza a sospensioni o interruzioni del servizio.

4. Riservatezza
4.1 L'accesso al servizio avviene mediante un codice di identificazione dell'utente (username) e una parola chiave (password). L'utente è informato del fatto che la conoscenza delle proprie credenziali da parte di terzi consentirebbe a questi ultimi l'utilizzo del servizio in nome dell'utente medesimo. L'utente è il solo ed unico responsabile della conservazione e della riservatezza delle proprie credenziali e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad essa connessi o correlati, (ivi compresi danni e conseguenze pregiudizievoli arrecati all'Università e/o a terzi) siano dal medesimo utente autorizzati ovvero non autorizzati.
4.2 L'utente si impegna a comunicare quanto prima all'Università l'eventuale furto, smarrimento o perdita della password. In ogni caso, resta inteso che l'utente sarà responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento di tale password.
4.3 L'utente prende atto ed accetta l'esistenza del registro dei collegamenti (noto come "log") mantenuto dell'Università, e l'Ateneo adotta misure tecniche ed organizzative necessarie a garantire la riservatezza di tale registro. Il registro dei collegamenti potrà essere esibito all'autorità giudiziaria, dietro esplicita richiesta.
4.3 L'utente prende atto ed accetta che le frequenze radio ed il traffico di rete wireless potranno essere sorvegliate allo scopo di mantenere le prestazioni della rete wireless ad un livello adeguato oltre che per garantire il corretto utilizzo del servizio.

5. Avvertenze

Le modalità tecniche d'uso della rete e le relative raccomandazioni sono pubblicate sul sito http://GENUAwifi.unige.it/

Letto e sottoscritto (L'utente) ……

(modello 9)

Al Centro Servizi Informatici e Telematici di Ateneo
Università degli Studi di Genova
Viale Cembrano, 4 – 16148 Genova
Tel. +39 10 353 2690
Fax +39 10 353 6518

Oggetto: Rete wifi dipartimentale

Il Responsabile della Struttura .....

- □ Notifica la presenza presso la propria struttura delle seguenti reti wifi, aventi le seguenti caratteristiche principali:……..
  ……...
  ……

- □ Richiede, presso la propria struttura/dipartimento:

  - □ Attivazione di una rete wifi
  - □ Supporto alla realizzazione di un progetto per reti wifi
  - □ La realizzazione di una rete wifi a fronte della disponibilita' economica dipartimentale di € ……..

- □ Verranno installati nr. …… AP, aventi le seguenti caratteristiche principali:
  ……...
  ……
  Gli AP che saranno gestiti dal personale tecnico dipartimentale secondo le correnti normative tecniche dell'Universita' di Genova.

Note:
…….
……

Il direttore ……..….

(modello 10)

Al Centro Servizi Informatici e Telematici di Ateneo
Università degli Studi di Genova
Viale Cembrano, 4 – 16148 Genova
Tel. +39 10 353 2690
Fax +39 10 353 6518

Oggetto: richiesta autorizzazione di accesso al servizio VPN

Da compilare a cura del Direttore del Dipartimento /Responsabile della Struttura:

Il sottoscritto.....

.....

Direttore del Dipartimento/Centro Universitario /Struttura .....

chiede che venga consentito l'accesso al servizio VPN ai seguenti dipendenti / collaboratori:

NOME e COGNOME .....

NOME e COGNOME .....

NOME e COGNOME .....

Data..... Firma.....

Recapito telefonico per eventuali comunicazioni.....

.....

(Allegato A)

ACCEPTABLE USE POLICY GARR[12]

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 cui si fa accesso.
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

[12] http://www.garr.it/reteGARR/aup.php?idmenu=collegare

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. È 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.