UNIVERSITÀ DEGLI STUDI DEL MOLISE

COORDINAMENTO AFFARI GENERALI
UFFICIO STATUTO, REGOLAMENTI ED ELEZIONI

IL RETTORE

VISTA La Legge 9 maggio 1989, n. 168, "Istituzione del Ministero dell'Università e della Ricerca Scientifica e Tecnologica";

VISTO il Documento approvato dalla Commissione Reti e Calcolo Scientifico del MURST in data 22 gennaio 1997 "Progetto di rete GARR a larga banda per le università e la ricerca scientifica italiana";

VISTO il D.L.vo 30 marzo 2001, n. 165, "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", ed in particolare l'art. 5, aggiornato al 22/06/2017, che demanda alle amministrazioni pubbliche ogni determinazione per l'organizzazione degli uffici al fine di perseguire obiettivi di efficienza, efficacia ed economicità garantendo l'imparzialità e la trasparenza dell'azione amministrativa;

VISTO il D.L.vo 29 dicembre 1992, n. 518, "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore";

VISTA la Legge 23 dicembre 1993, n. 547, "Modificazioni ed integrazioni alle norme del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica";

VISTO il D.L.vo 12 febbraio 1993, n. 39, e succ. modif. "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche";

VISTA la normativa sull'archiviazione sostitutiva in particolare il D.P.R. n. 445/2000 e succ. modif. "Testo unico delle disposizioni legislative e regolamentari in maniera di documentazione amministrativa"; la Deliberazione CNIPA n. 11/2004 Note esplicative "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali";

VISTA la normativa sulla Posta elettronica e sulla Posta elettronica certificata (PEC) in particolare la Direttiva della Presidenza del Consiglio dei Ministri del 27 novembre 2003 "Impiego della posta elettronica nelle pubbliche amministrazioni", il Decreto Presidente della Repubblica n. 68/2005 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.", il Decreto Presidenza del Consiglio dei Ministri del 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata", nonché il provvedimento del 10 marzo 2007 del Garante per la protezione dei dati personali "Le linee guida del Garante per la posta elettronica e internet";

VISTA la normativa sull'accessibilità in particolare la Legge 9 gennaio 2004, n. 4, "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici", il D.P.R. 1° marzo 2005, n. 75, "Regolamento di attuazione della legge 9 gennaio 2004, n. 4 per favorire l'accesso dei soggetti disabili agli strumenti informatici" e il D.M. 8/7/2005 "Requisiti tecnici e i diversi livelli per l'accessibilità agli strumenti informatici";

VISTO il "Codice dell'amministrazione digitale" (D.L. n. 82/2005) e successive modifiche ed integrazioni (D.L. n. 159/2006, L. 244/2007, D.L. n. 185/2008, L. 69/2009; L. 102/2009, D.L. 235/2010, D.L. 179/2012, L. 190/2014, D.L. 179/2016, D.L. 217/2018);

VISTA la Direttiva del Ministro per l'innovazione e le tecnologie 27/7/2005 "Qualità dei servizi on line e misurazione della soddisfazione degli utenti";

VISTA la delibera del Consiglio di Amministrazione del 31/1/2001 con la quale sono stati designati il referente tecnico e amministrativo (APM, Access Point Manager e APA, Access Point Administrator) dell'Università degli Studi del Molise per la gestione della rete GARR;

VISTO il Regolamento Generale di Ateneo, in particolare, il Titolo II "Norme relative all'organizzazione amministrativa e al funzionamento degli uffici";

VISTE le delibere del S.A. e del C.d.A. sul sistema di Controllo di gestione per verificare l'efficacia, l'efficienza e l'economicità dell'azione amministrativa al fine di ottimizzare il rapporto tra costi e risultati;

CONSIDERATO che l'Università degli Studi del Molise promuove l'utilizzazione della Rete Dati di Ateneo, quali strumento utile, compatibilmente con le proprie strutture e risorse, a perseguire le proprie finalità istituzionali, di didattica e di ricerca;

RITENUTO pertanto, opportuno realizzare un documento informativo che stabilisce le condizioni e le modalità vincolanti per l'accesso e l'utilizzazione della Rete Dati di Ateneo e delle risorse informatiche e allo stesso tempo regolamenta l'attività della

VISTO il D.R. n. 1970 del 22 dicembre 2008 con il quale è stato emanato il Regolamento per l'utilizzo delle risorse informatiche dell'Università degli Studi del Molise;

VISTA la delibera del Senato Accademico adottata nella seduta del 20 aprile 2018;

VISTA la conforme delibera del Consiglio di Amministrazione adottata nella seduta del 20 aprile 2018;

DECRETA

Art. 1 – E' emanato il "Regolamento per l'accesso e l'utilizzo delle risorse e dei servizi informatici dell'Università degli Studi del Molise", e relativo allegato, il cui testo è allegato al presente provvedimento di cui fa parte integrante (Allegato A) che annulla e sostituisce il Regolamento emanato con D.R. n. 1970 del 22 dicembre 2008.

Art. 2 – Il Regolamento di cui all'art. 1 entra in vigore dal giorno 1° luglio 2018.

IL RETTORE
Prof. Gianmaria PALMIERI

(Documento informatico sottoscritto con firma digitale ai sensi del D.Lvo n. 82/2005, s.m.i. e norme collegate)

Allegato "A" al D.R. n. 515 *del* 22 GIU. 2018

Regolamento per l'accesso e l'utilizzo delle risorse e dei servizi informatici dell'Università degli Studi del Molise

Art. 1 - Finalità e ambito di applicazione

Il presente Regolamento stabilisce le condizioni e le modalità vincolanti per l'accesso e l'utilizzo delle risorse, dei servizi informatici e della Rete Informatica e Telematica dell'Università degli Studi del Molise, in seguito indicata come Rete dati di Ateneo.

L'Università degli Studi del Molise, consapevole delle potenzialità offerte dagli strumenti informatici e telematici, promuove l'utilizzo delle risorse e dei servizi informatici di Ateneo, con l'intento di perseguire le proprie finalità nel quadro dell'attività istituzionale e amministrativa, dell'attività didattica e di ricerca.

L'accesso e l'utilizzo delle risorse e dei servizi informatici comporta l'integrale e incondizionata accettazione delle norme del presente Regolamento e il rispetto della normativa vigente in materia.

L'Area Servizi Informatici è la struttura preposta alla gestione tecnica dei servizi informatici e telematici.

Art. 2 - Definizioni

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

- *Backup:* meccanismo per la conservazione di materiale informativo su un supporto di memorizzazione per prevenire la perdita totale dei dati archiviati nella memoria di massa dei computer;
- *Credenziali di accesso*: dati utilizzati nelle operazioni di autenticazione utente (per es. nome utente e password);
- *GARR*: Gruppo Armonizzazione Reti per la Ricerca;
- *Host (terminale informatico)*: ogni dispositivo ad esempio computer, stampante, periferica, telefono, fax, ecc., connesso alla Rete Dati di Ateneo;
- *IP (Internet Protocol)*: numero che identifica univocamente un host nella Rete Dati di Ateneo;
- *Log:* file o insieme di file contenenti le registrazioni di operazioni compiute durante l'utilizzo di un servizio di rete nonché la registrazione dei dati necessari all'identificazione dei responsabili di tali operazioni;
- *Malware:* software creato con lo scopo di causare danni più o meno gravi ai dati degli utenti, o a un sistema informatico;
- *Presa utente interna*: punto di connessione fonia/dati (nodo terminale), al quale può essere collegato un Host;
- *Referenti di struttura:* personale dell'università che costituisce l'interfaccia amministrativa e tecnica dell'utenza verso l'Area Servizi Informatici;
- *Responsabili di struttura*: i responsabili di Area e dei Settori, dei Dipartimenti, dei Centri, dei laboratori o di altre strutture organizzative;
- *Rete dati di Ateneo*: insieme delle infrastrutture fisiche e logiche che consentono la comunicazione e

la trasmissione dati e fonia sia all'interno che all'esterno dell'Ateneo;

- *Risorse informatiche:* qualsiasi tipo di *hardware* (computer, modem, stampante, scanner, videoterminali, ecc...), *software, dati e informazioni in formato elettronico*, di proprietà o comunque nella disponibilità dell'Università o ad essa concessi in licenza d'uso;
- *Servizi informatici*: servizi che utilizzano la Rete Dati di Ateneo e che sono erogati dall'Area Servizi Informatici a beneficio dell'Ateneo (ad esempio accesso ad Internet, Posta Elettronica, sito web di Ateneo);
- *Spam*: messaggi di posta elettronica indesiderati;
- *Utente*: qualsiasi persona o struttura autorizzata che accede ai servizi informatici dell'Università degli Studi del Molise.

Art. 3 - Risorse informatiche

Le *risorse informatiche* possono essere utilizzate esclusivamente per assolvere alle finalità proprie dell'Università, per l'attività didattica, scientifica e tecnico-amministrativa.

Ogni utente è tenuto ad adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle *risorse informatiche*.

È vietato installare o prelevare software, copiare file eseguibili, file musicali, giochi sia sui dischi di rete sia su quelli locali senza autorizzazione. Per utilizzare programmi diversi da quelli già installati occorre rivolgersi all'Area Servizi Informatici.

Gli utenti sono tenuti ad utilizzare correttamente le apparecchiature, al fine di evitare qualsiasi danneggiamento delle *risorse informatiche*.

Art. 4 - Accesso alla Rete dati di Ateneo e ai servizi informatici

Per il periodo di tempo necessario all'espletamento dei loro compiti all'interno dell'Ateneo possono accedere alla *Rete dati di Ateneo* e ai relativi servizi informatici:

a) i professori, i ricercatori, il personale tecnico-amministrativo dell'Università e i tecnici a contratto;
b) gli studenti regolarmente iscritti all'Università e quelli dei programmi Erasmus;
c) i partecipanti a seminari o convegni gestiti o organizzati dall'Università anche in compartecipazione con altri enti con i quali esistono apposite convenzioni;
d) i titolari di borse di studio, gli assegnisti di ricerca, i collaboratori alla ricerca e alla didattica, i componenti degli organi dell'Università ancorché non dipendenti dell'Università;
e) i dottorandi di ricerca;
f) gli utenti delle organizzazioni che aderiscono alla federazione eduroam.

Nelle convenzioni tra l'Ateneo ed altri Enti pubblici o privati può essere previsto l'*accesso alla Rete dati di Ateneo* limitatamente agli appartenenti agli Enti in questione che partecipano alle attività oggetto delle convenzioni, e per le attività ad esse relative.

Potrà essere autorizzato, caso per caso, l'accesso a singoli utenti che non rientrano nelle categorie sopra elencate.

Ogni utilizzatore della rete è tenuto ad adottare le necessarie misure di sicurezza e comportamenti adeguati per non interferire con il corretto funzionamento delle comunicazioni e per garantire l'integrità dei sistemi e l'accesso alle risorse da parte di altri utenti.

L'Ateneo può bloccare o limitare l'accesso alla *Rete dati* e/o ai *servizi informatici* da parte di un *Host*, al fine di preservare il buon funzionamento della *Rete Dati di Ateneo* nella sua globalità.

Art. 5 - Posta elettronica istituzionale

L'Università degli Studi del Molise, nell'ambito delle proprie attività, fermo restando l'osservanza delle norme in materia di riservatezza dei dati personali e delle norme tecniche di sicurezza informatica, si adopera per estendere la diffusione e l'utilizzo degli strumenti telematici in sostituzione dei canali tradizionali di comunicazione.

Sono abilitati a ricevere una casella di posta elettronica istituzionale (@unimol.it) gli utenti indicati nell'art. 4 comma 1 punti *a* e *d.* È altresì possibile attivare apposite caselle istituzionali di tipo *non personale* affidate alla responsabilità delle strutture di competenza. Per gli utenti indicati nell'art. 4 comma 1 punti *b* ed *e* si rinvia allo specifico "*regolamento per il servizio di posta elettronica rivolto agli studenti*".

Gli utenti sono invitati a consultare la propria casella di posta elettronica istituzionale periodicamente.

A seguito della cessazione del rapporto contrattuale con l'Ateneo, la casella di posta elettronica rimarrà attiva per tre mesi al fine di consentire all'utente l'eventuale backup dei dati e l'eventuale comunicazione ai corrispondenti dell'imminente cancellazione della stessa.

L'Amministrazione si riserva di:

- sospendere gli account di posta elettronica che vengono utilizzate per l'invio di e-mail che contengono *malware* o *spam*;
- effettuare i necessari controlli su eventuali utilizzi, consapevolmente impropri del servizio di posta elettronica, ricorrendo, ove necessario, alle autorità competenti.

Art. 6 - Modalità di accesso ai servizi informatici

Per poter accedere ai servizi informatici gli utenti abilitati devono utilizzare le procedure relative al singolo servizio:

- *Accesso alla Rete dati da parte degli utenti abilitati (art. 4)*

  Le credenziali di accesso alla Rete Dati vengono rilasciate dall'Area Servizi Informatici, a seguito della compilazione dell'apposito modulo, pubblicato sul sito unimol.it, debitamente compilato ed autorizzato dalla struttura alla quale l'interessato afferisce o ha relazioni di ricerca, didattica o studio.

- *Accesso alla rete wi-fi da parte degli ospiti*

  Per consentire agli *ospiti* di poter accedere alla rete wi-fi di ateneo è necessario che il *responsabile della struttura* ospitante faccia pervenire 14 giorni prima dell'evento la richiesta all'Area Servizi Informatici attraverso l'apposito modulo pubblicato sul sito unimol.it.

- *Accesso alla rete wi-fi da parte degli utenti della federazione Eduroam*

  È consentito agli utenti appartenenti ad organizzazioni che hanno aderito alla Federazione Eduroam l'accesso alla rete wifi utilizzando le metodologie di autenticazione definiti dalla federazione stessa.

- *Assistenza informatica rivolta agli utenti interni*

  Per accedere al servizio di supporto e assistenza è necessario utilizzare il servizio web disponibile all'indirizzo http://assistenza.unimol.it ed accessibile esclusivamente dalla *rete dati di Ateneo*.

  Il servizio è attivo per il personale docente e tecnico-amministrativo.

- *Assistenza informatica rivolta agli studenti*

  Per le richieste di assistenza informatica relative ai servizi a disposizione degli *studenti* (ad esempio posta elettronica istituzionale, rete dati di ateneo, portale dello studente, ecc.) è necessario inviare una richiesta all'indirizzo assistenza@studenti.unimol.it o rivolgersi personalmente ai *Referenti di struttura*.

- *Attivazione casella di posta elettronica istituzionale*

  Le credenziali di accesso alla casella di posta elettronica vengono rilasciate dall'Area Servizi Informatici, a seguito della compilazione dell'apposito modulo, pubblicato sul sito unimol.it, debitamente compilato ed autorizzato dalla struttura alla quale l'interessato afferisce o ha relazioni di ricerca, didattica o studio.

  Per rinnovare la validità della casella di posta elettronica istituzionale, assegnata agli utenti con contratti a termine, le strutture amministrative di competenza devono inviare periodicamente un elenco aggiornato all'Area Servizi Informatici, con la nuova durata contrattuale.

- *Richieste di hosting web (portali per progetti di ricerca, forum, e-learning)*

  Per richiedere l'attivazione di hosting web è necessario effettuare la richiesta attraverso l'apposito modulo pubblicato sul sito unimol.it, da compilare in ogni sua parte e consegnare all'Area Servizi Informatici.

  Per rinnovare la validità del servizio le strutture richiedenti devono inviare il modulo per il rinnovo del servizio almeno un mese prima della scadenza precedentemente indicata.

Art. 7 - Responsabili di struttura

I *responsabili di struttura* dovranno adottare misure idonee per un corretto utilizzo delle *risorse informatiche* messe a disposizione della loro struttura, esercitando una funzione di indirizzo e controllo e definendo le responsabilità per la gestione dei dati e delle risorse stesse, nonché per la concessione eventuale di password di accesso alle banche dati gestite dalla struttura di appartenenza.

Art. 8 - Modalità di connessione degli Host alla Rete dati di Ateneo

Per poter connettere un qualunque *Host* alla rete cablata di Ateneo, il *Referente di struttura* o l'*Utente*, deve richiedere la specifica autorizzazione e gli appositi dati di configurazione all'Area Servizi Informatici.

Art. 9 - Responsabilità e obblighi dell'utente

L'utilizzo dei *servizi informatici* e delle *risorse informatiche* è subordinato al rispetto da parte dell'utente della normativa vigente, del presente Regolamento, oltre che delle norme che regolano la Rete *GARR (*Acceptable Use Policy) presenti sul sito www.garr.it.

Pertanto l'utente si impegna:

- ad osservare il presente Regolamento;

- a rispettare la normativa vigente, le norme GARR ed eventuali altre regole che disciplinano le attività e i servizi che utilizzano la Rete dati di Ateneo;

- ad acconsentire al trattamento dei suoi dati personali necessari per l'erogazione del servizio e dei log da parte dell'Ateneo, in conformità alle norme legislative e regolamentari vigenti.

L'utente inoltre deve essere a conoscenza che:

- l'utente è responsabile delle attività svolte nella Rete dati di Ateneo;

- l'utente è responsabile per eventuali difformità riscontrate sulle apparecchiature assegnate;

- la modifica dell'indirizzo IP e del MAC ADDRESS è espressamente vietata;

- le credenziali di accesso sono personali e non possono essere condivise o cedute;

- l'utente è responsabile per la protezione dei dati utilizzati e/o memorizzati nei sistemi a cui ha accesso ed è tenuto ad adottare tutte le misure necessarie ai sensi della normativa vigente;

- l'utente è tenuto a mantenere aggiornato il software antivirus installato sull'*Host* utilizzato;

- l'utente è responsabile del contenuto dei materiali prodotti e diffusi attraverso la rete dallo stesso;

- l'utente è obbligato a segnalare immediatamente all'Area Servizi Informatici o *al Referente di struttura* ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;

- l'utente è tenuto a mantenersi aggiornato, controllando periodicamente le direttive dell'Area Servizi Informatici.

A titolo esemplificativo e non esaustivo, è vietato:

1. utilizzare la Rete Dati di Ateneo per accedere a risorse di rete di cui non si dispone dell'autorizzazione;
2. fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso alla Rete dell'Università;
3. usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi; l'Area Servizi Informatici si riserva la facoltà di impedire in qualsiasi momento l'accesso alla Rete di Ateneo da parte di utenti anonimi o non identificati;
4. violare gli obblighi in materia di copyright o utilizzare software di cui non si dispone della licenza d'uso, compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
5. svolgere attività che causano malfunzionamento, influiscono negativamente la regolare operatività, danneggiano o riducono considerevolmente l'utilizzabilità o le prestazioni della Rete dati di Ateneo;
6. manomettere in qualsiasi modo le apparecchiature e le strutture informatiche ed elettroniche dell'Ateneo;
7. violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete dati d'Ateneo, dei quali non si è destinatari specifici;

8. distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare o accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili;
9. diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno;
10. utilizzare la Rete dati di Ateneo e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale;
11. installare apparati di rete senza la preventiva autorizzazione dell'Area Servizi Informatici;
12. accedere ai locali e ai box riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi senza l'autorizzazione dell'Area Servizi Informatici;
13. copiare (a meno che la licenza d'uso non lo consenta) e/o utilizzare i programmi messi a disposizione dall'Amministrazione per installazioni esterne;
14. installare sui personal computer di proprietà dell'Amministrazione qualunque tipo di software e di hardware, anche se dotato di licenza d'uso, senza che l'amministrazione ne sia a conoscenza e ne abbia dato il consenso al fine di permettere il corretto funzionamento della singola postazione o dell'intera rete.

Art. 10 - Modalità per l'erogazione di servizi informatici

I soggetti autorizzati ad accedere alla Rete dati di Ateneo possono erogare tramite essa dei servizi informatici. Tali servizi dovranno essere conformi al presente regolamento ed ai regolamenti emanati dal *GARR* e dovranno essere autorizzati dall'Area Servizi Informatici.

L'Area Servizi Informatici può bloccare o limitare temporaneamente l'erogazione di tali servizi da parte di un Host, al fine di preservare il buon funzionamento della *Rete Dati di Ateneo* nella sua globalità.

Art. 11 - Ruolo dell'Area Servizi Informatici

L'Università degli Studi del Molise ha affidato all'*Area Servizi Informatici* la gestione tecnica della Rete dati di Ateneo, dei servizi informatici e telematici dell'Ateneo.

L'*Area Servizi Informatici* assicura in modo esclusivo il monitoraggio, l'aggiornamento ed ampliamento della Rete dati di Ateneo sia sotto l'aspetto fisico che logico, curandone i relativi progetti.

L'*Area Servizi Informatici* nell'espletamento delle proprie attività di gestione e monitoraggio della Rete di Ateneo:

1) è titolare del trattamento dei dati di log relativi alle attività di rete dei singoli host (flussi generati, richieste DNS, indirizzi IP, servizi erogati sulla rete);
2) ha la facoltà di revocare le credenziali di accesso ai servizi e/o l'autorizzazione di accesso alla Rete Dati di Ateneo da parte di un Host, o limitare la fruizione di servizi da parte dello stesso, a fronte di:

   - violazioni del presente regolamento o della normativa vigente applicabile;

- di erogazione di servizi potenzialmente dannosi per un buon funzionamento delle Rete dati di Ateneo nel suo complesso;

3) ha la facoltà di bloccare la consultazione di siti Web, Newsgroups e altre risorse su richiesta dell'Amministrazione.

Art. 12 - Utilizzo dei Nomi a Dominio

Il dominio DNS unimol.it e tutti i sottodomini sono gestiti dall'*Area Servizi Informatici* nell'interesse dell'Ateneo.

Art. 13 - Aule informatiche

Le norme contenute nel presente regolamento si applicano anche alle aule informatiche dell'Università degli Studi del Molise.

Il referente tecnico addetto all'aula disciplinerà l'accesso alla stessa e l'uso delle apparecchiature informatiche assegnate.

Art. 14 - Violazioni

L'*Area Servizi Informatici* può disattivare in qualsiasi momento un codice d'accesso personale e/o una password, disconnettere un *Host*, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento della *Rete Dati di Ateneo*, oppure qualora vi sia fondato sospetto che l'Utente abbia violato il presente Regolamento.

L'*Area Servizi Informatici* ha la facoltà di informare gli Organi competenti dell'Ateneo a fronte di comportamenti in violazione del presente regolamento o se vi sia il fondato sospetto che ciò sia avvenuto.

La revoca permanente dell'autorizzazione di accesso alla *Rete Dati di Ateneo*, da parte di uno o più Host, dovrà essere disposta dal Direttore Generale su proposta dell'Area Servizi Informatici.

Sono fatte salve le ulteriori conseguenze di natura penale, civile, amministrativa e disciplinare della violazione compiuta. In particolare, si rammenta che i comportamenti illeciti che integrano gli estremi di reato sono perseguibili dall'autorità giudiziaria e puniti a norma della legge penale.

Consortium GARR

Allegato

Versione approvata dal
CdA GARR del 28/07/2014

Acceptable Use Policy - AUP

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, e gli altri servizi ad esso correlati, sono destinati 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 e dei suoi servizi 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, di storage, di calcolo e di tutti quegli 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, 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, storage o calcolo, 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 o immagazzinare (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, 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 ed i suoi servizi è delle persone che li producono e diffondono. Nel caso di persone che non hanno raggiunto la maggiore età, la responsabilità può coinvolgere anche le persone che la legge indica come tutori dell'attività dei minori.

5. I soggetti autorizzati (S.A.) all'accesso alla Rete GARR, definiti nel documento "Regole di accesso alla Rete GARR", possono utilizzare la Rete ed i suoi servizi 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 Consortium GARR.

6. Tutti gli utenti a cui vengono forniti accessi alla Rete GARR ed ai suoi servizi devono essere riconosciuti ed identificabili. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati. Di norma gli utenti devono essere dipendenti del soggetto autorizzato, anche temporaneamente, all'accesso alla Rete GARR.

Per quanto riguarda i soggetti autorizzati all'accesso alla Rete GARR (S.A.) gli utenti possono essere anche persone temporaneamente autorizzate da questi in virtù di un rapporto di lavoro a fini istituzionali. Sono utenti ammessi gli studenti regolarmente iscritti ad un corso presso un soggetto autorizzato con accesso alla Rete GARR

7. E' responsabilità dei soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR di adottare tutte le azioni ragionevoli per assicurare la conformità delle proprie norme con quelle qui esposte e per assicurare che non avvengano utilizzi non ammessi della Rete GARR. Ogni soggetto con accesso alla Rete GARR deve inoltre portare a conoscenza dei propri utenti (con i mezzi che riterrà opportuni) le norme contenute in questo documento.
8. I soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR ed ai suoi servizi 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 e dei suoi servizi, 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 ed ai suoi servizi è condizionato all'accettazione integrale delle norme contenute in questo documento.