Università degli Studi - L'Aquila

Area Informatica Infrastrutture Reti e Web

Settore Reti e Sicurezza

Modulo Richiesta Utente Esterno

_____ lì _____
Rep. n. _____ - Prot. n._____ Allegati ___
Anno_____ tit. ___ cl. ___ fasc. ___

Il presente modulo, dopo essere stato debitamente compilato, firmato e protocollato, deve essere inviato al Settore Reti e Sicurezza, o per e-mail con scansione in pdf all'indirizzo: reti@strutture.univaq.it, o per posta all'indirizzo Università degli Studi dell'Aquila – ARINRE - Settore Reti e Sicurezza - via Vetoio – Coppito, 67100 L'Aquila, oppure via FAX al numero: 0862431218.

Nome:_____ Cognome:_____

Codice Fiscale:_____ n° Telefono/Cellulare_____

Indirizzo e-mail (non UNIVAQ):_____

Tipologia rapporto di lavoro con l'Università: _____

Data fine rapporto: _____ (Se non indicato l'account avrà validità 6 mesi)

Campi da far compilare dal referente interno di Ateneo:

Nome:_____ Cognome:_____

Codice Fiscale: _____ Struttura di appartenenza:_____

Firma: _____

Servizi Richiesti:

☐ Accesso rete wifi	☐ Accesso Vpn
☐ Accesso Rete cablata	☐ Account posta elettronica dominio: @guest.univaq.it

_____ lì _____

Firma

_____

Allegato1: Fotocopia del proprio documento di identità (debitamente firmato)
Allegato2: Fotocopia del proprio Codice Fiscale
N.B. In assenza dei documenti allegati la richiesta non sarà presa in considerazione.

Estratto del Regolamento
"Norme relative all'accesso ed all'uso della rete informatica"

Emanato con Decreto Rettorale n. 1092-2005 del 30.03.2005
Rettificato con Decreto Rettorale n. 1313-2005 del 12.04.2005
Modificato con D.R. n. 1936/2012 del 20.08.2012

Art. 5 - Monitoraggio e controllo

1. Il Dipartimento Gestione Servizi Informatici e/o le strutture informatiche dipartimentali:
   a) esercitano una attività di monitoraggio e controllo sul corretto e ottimale funzionamento delle risorse di rete, intervenendo per il pronto ripristino in presenza di eventuali guasti tecnici sugli apparati di rete;
   b) in caso di anomalie, imputabili a un uso improprio della rete o a un malfunzionamento di sistemi a essa collegati, intervengono avvisando tempestivamente l'utente responsabile richiedendo la pronta cessazione delle cause e il ripristino del buon funzionamento;
   c) provvedono a escludere e/o limitare l'utilizzo delle risorse di rete, in caso del persistere delle anomalie e in caso di attività e/o condizioni che compromettano il funzionamento della rete stessa, fino alla cessazione delle cause;
   d) collaborano al ripristino del corretto funzionamento delle reti di competenza.
2. Tutti gli utenti:
   a) esercitano una attività di monitoraggio e controllo sui sistemi di propria competenza, impegnandosi ad adottare ogni precauzione necessaria al funzionamento ottimale dei sistemi medesimi;
   b) si impegnano a dotarsi di misure atte a contrastare la diffusione di virus, hoaxes o altri programmi che possano danneggiare, molestare o perturbare le attività di altre persone, utenti o servizi disponibili sulla rete di Ateneo, sulla rete GARR e su altre reti a essa collegate;
   c) si impegnano a non concedere a terzi le proprie credenziali per l'accesso alla rete e ai servizi tramite essa fruibili.

Art. 6 - Attività vietate

1. È vietato usare la rete:
   a) in modo difforme da quanto previsto nel presente regolamento;
   b) in modo difforme dalle regolamentazioni dettate dai responsabili della rete GARR;
   c) in modo difforme da quanto previsto dalle leggi penali, civili e amministrative, nazionali e internazionali, in materia di disciplina delle attività e dei servizi svolti sulla rete.
   d) per scopi incompatibili con le finalità e con l'attività istituzionale dell'Ateneo così come stabilito nello Statuto e nel codice etico dell'Università;
   e) per conseguire l'accesso illecito a risorse di rete interne o esterne all'Ateneo;
   f) per utilizzare impropriamente servizi o risorse di rete, o collegare a essa apparecchiature o software, o installare programmi di fonte ignota senza preventivo controllo e autorizzazione dell'Amministrazione, o comunque programmi non funzionali alla prestazione lavorativa;
   g) per la promozione o diffusione di iniziative pubblicitarie, per attività di carattere commerciale o per propaganda;
   h) per la conduzione di ricerche non rientranti nelle proprie mansioni e funzioni;
   i) per creare, trasmettere o scaricare volontariamente messaggi, immagini, dati o materiale offensivo, diffamatorio, osceno, discriminante o che comunque attenti ai diritti assoluti della persona e alla dignità umana;
   j) per danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti;
   k) per ostacolare, attraverso abusi che depauperano le risorse di rete, la regolare operatività della stessa, restringendone o rallentandone le potenzialità a discapito della piena fruibilità da parte degli utenti;
   l) per attività che distraggano risorse (persone, capacità, elaboratori);
   m) per attività che provochino trasferimenti illeciti di informazioni;
   n) per attività che violino le leggi a tutela delle opere dell'ingegno;
   o) è inoltre vietato usare l'anonimato o servirsi di risorse che consentano di restare anonimi, nonché alterare la propria identità.

Art. 7 - Sanzioni

1. In caso di abuso, a seconda della gravità del medesimo, e fatte salve le ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le seguenti sanzioni:
   a) La limitazione, anche totale, dall'accesso alla rete da un minimo di una settimana a un massimo di sei mesi;
   b) L'esclusione definitiva dall'uso della rete.
2. Le sanzioni sono comminate dal Direttore Generale su proposta di un apposito Comitato (vedi art. 8) o, nelle more della relativa costituzione, su proposta del Dipartimento Gestione Servizi Informatici e/o del Direttore del Dipartimento competente.
3. In caso abbia notizia di abuso e vi sia pericolo nel ritardo il Rettore può ordinare l'immediata cessazione dell'attività all'origine dell'abuso adottando le necessarie misure per impedire che l'abuso venga portato a ulteriori conseguenze.