

Al Responsabile dell' Area Servizi Informatici
Università degli Studi Magna Græcia di
Catanzaro

**Oggetto: Richiesta di attivazione/rinnovo vpn
sistema UNICZ.IT**

Il richiedente: __

Qualifica:

Dipartimento/Struttura:

Codice fiscale:

Tel Uff.:

Indirizzo mail:

CHIEDE

attivazione VPN

rinnovo VPN

a far data dal

Durata certificato un Anno

Nominativo del Responsabile del Corso/Scuola/Dipartimento UMG[1]:

Il richiedente si IMPEGNA

a non utilizzare login ed accessi v p n per scopi diversi da quelli della sua Struttura di appartenenza e a non cederli per alcun motivo ad altri. Il/la sottoscritto/a si impegna a rispettare quanto sancito dalle Regole del GARR che consentono l'accesso alla ree GARR esclusivamente per scopo di ricerca e/o istituzionale.

Il/la richiedente si impegna **a non memorizzare la password di sblocco dei certificati** che consentono l'utilizzo della VPN.

Motivazione della richiesta _____

Indirizzo Ip Computer Ateneo _____

Applicazioni da raggiungere _____

Ogni soggetto che, mediante VPN, si collega all'Ateneo UMG di Catanzaro assume piena e personale responsabilità delle attività svolte attraverso i certificati e la password a lui assegnati.

Il modello compilato dovrà essere inoltrato all'indirizzo mail **vpn@unicz.it** e, **solo nel caso di Personale non strutturato**, per cc alla mail del Responsabile del Corso/Scuola/Dipartimento UMG su indicato

Il/La richiedente sono autorizzati ad utilizzare per il collegamento i Personal Computer personali a condizione che vengano garantite come minimo le seguenti misure:

- utilizzare sistemi operativi per i quali attualmente è garantito il supporto;
- effettuare costantemente gli aggiornamenti di sicurezza del proprio sistema operativo;
- assicurarsi che i software di protezione del proprio sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati;
- assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dall'ASI dell'Università UMG di Catanzaro;
- non installare software proveniente da fonti/repository non ufficiali;
- non cliccare su link o allegati contenuti in e-mail sospette;
- utilizzare l'accesso a connessioni Wi-Fi solo se adeguatamente protette;
- non utilizzare dispositivi mobili (pen-drive, hdd-esterno, ecc.);
- effettuare sempre il log-out dai servizi/portali utilizzati dopo che si è conclusa la sessione lavorativa.

Inoltre Il/La richiedente si impegna a:

- 1) Accedere esclusivamente ai servizi e ai sistemi informativi per i quali sono stati espressamente autorizzati e con le modalità consentite;
- 2) Garantire, sotto la propria personale responsabilità, il mantenimento della necessaria riservatezza sulle proprie credenziali e certificati;
- 3) Comunicare immediatamente al Referente del sistema informatico lo smarrimento, il furto o l'appropriazione da parte di terzi delle proprie credenziali;
- 4) Segnalare immediatamente qualsiasi incidente o malfunzionamento dei sistemi di collegamento in VPN;
- 5) Bloccare la propria postazione informatica in tutte le occasioni in cui ci sia necessità di allontanamento anche temporaneo dalla stessa.
- 6) Non recar danno o pregiudizio ai dati e/o ai software in uso agli uffici e a non interferire con l'utilizzo dei servizi di rete da parte di altri utenti;
- 7) Rispettare le norme contenute nel presente regolamento accesso VPN e ad utilizzare le credenziali assegnate ai soli fini di fruizione dei servizi a cui sono stati autorizzati.
- 8) Non condividere le proprie credenziali e certificati con terzi per nessuna motivazione.
- 9) Disconnettere immediatamente la connessione VPN non appena terminate le attività lavorative necessarie.
- 10) Rispettare la vigente normativa posta a tutela della riservatezza e dei dati personali. Ogni soggetto che, mediante VPN, si collega ai sistemi dell'Università UMG di Catanzaro assume piena e personale responsabilità delle attività svolte attraverso le credenziali e i certificati a lui assegnati.
- 11) Custodire le propri credenziali e i propri certificati in modo sicuro sotto la propria responsabilità.

Data _____

Firma _____

PARTE RISERVATA ALL'UFFICIO (da non compilare)

Username attivato: _____ Password attiva: _____

Data attivazione: _____

Eventuali Note: _____

Il Sistemista