UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
DR/2019/4754 del 22/11/2019
Firmatari: De Vivo Arturo

U.S.R.

IL RETTORE

VISTO il vigente Statuto di Ateneo;
VISTO il D.P.R. 10 novembre 1997, n. 513, relativo al "*Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo15, comma 2, della legge 15 marzo 1997, n. 59*";
VISTO il D.P.R. 28 dicembre 2000, n. 445, recante il "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*";
VISTO il D.Lgs. 23 gennaio 2002, n. 10, riguardante l'"*Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche*";
VISTO il D.P.R. 11 febbraio 2005, n. 68, concernente il "*Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3*";
VISTO il D.Lgs. 28 febbraio 2005, n. 42, concernente l'"*Istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione, a norma dell'articolo 10, della legge 29 luglio 2003, n. 229*"**;**
VISTO il D.Lgs. 7 marzo 2005, n. 82, e ss.mm.ii., recante il "*Codice dell'Amministrazione Digitale"*;
VISTO il D.Lgs. 24 gennaio 2006, n. 36, riguardante l'"*Attuazione della direttiva 2003/98/CE relativa al riutilizzo di documenti nel settore pubblico*";
VISTO il *Regolamento di Ateneo in materia di firma digitale*, emanato con D.R. n. 4064 del 31/10/2006;
VISTO il *Regolamento per l'utilizzo del servizio di Posta elettronica@unina.it*, emanato con D.R. n. 4489 del 29/12/2010;
VISTO il *Regolamento per l'utilizzo del servizio di Posta elettronica@studenti.unina.it*, emanato con D.R. n. 4488 del 29/12/2010;
VISTO il *Regolamento di Ateneo in materia di Posta Elettronica Certificata*, emanato con D.R. n. 1614 del 11/05/2012;
VISTE le regole che disciplinano la Rete Italiana dell'Università e della Ricerca, denominata comunemente "Rete GARR" - di cui questo Ateneo è parte - e, in particolare, dell'*Acceptable Use Policy (AUP)* nella versione approvata dal CdA GARR il 6 novembre 2017;
RITENUTO necessario adottare un regolamento che disciplini le condizioni e le modalità per l'accesso e l'utilizzazione della Rete Informatica e Telematica di Ateneo e dei Servizi ad essa strettamente collegati, quale strumento utile a perseguire le proprie finalità istituzionali di didattica, ricerca, terza missione e l'efficienza dei propri servizi amministrativi nonché di tutte le attività istituzionali dell'Università;
VISTA la Delibera n. 28 del 24/10/2019 con la quale il Senato Accademico ha approvato, subordinatamente al parere del Consiglio di Amministrazione, il *Regolamento sull'accesso e l'utilizzazione della rete informatica e telematica dell'Ateneo*;
VISTA la Delibera n. 76 del 24/10/2019 con la quale il Consiglio di Amministrazione ha espresso parere favorevole in merito al sopra citato *Regolamento sull'accesso e l'utilizzazione della rete informatica e telematica dell'Ateneo*,

DECRETA

E' emanato nel testo allegato al presente Decreto, di cui costituisce parte integrante e sostanziale, il *Regolamento sull'accesso e l'utilizzazione della rete informatica e telematica dell'Ateneo*.
Il sopra citato Regolamento entra in vigore il giorno successivo a quello della sua pubblicazione all'Albo Ufficiale dell'Ateneo.

IL RETTORE
Gaetano MANFREDI

Ripartizione *Affari Generali*
Il Dirigente della Ripartizione *dott. Giuseppe Festinese*
Unità organizzativa responsabile del procedimento:
Ufficio Statuto, Regolamenti e Organi Universitari
Responsabile del procedimento:
Il Capo dell'Ufficio *dott. Antonio Nasti*

AdP

UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

REGOLAMENTO SULL'ACCESSO E L'UTILIZZAZIONE DELLA RETE

INFORMATICA E TELEMATICA DI ATENEO

Art. 1: Oggetto e ambito di applicazione

L'Università degli Studi di Napoli "Federico II", in seguito indicata come Università, consapevole delle potenzialità offerte dagli strumenti informatici e telematici, promuove l'utilizzazione della Rete Informatica e Telematica di Ateneo, in seguito Rete, quale strumento utile a perseguire le proprie finalità istituzionali di didattica, ricerca, terza missione, e l'efficienza dei propri servizi amministrativi.

Il presente Regolamento stabilisce le condizioni e le modalità per l'accesso e l'utilizzazione della Rete di Ateneo e dei Servizi ad essa strettamente collegati -DNS, VPN, Proxy- agli utenti interni ed esterni. L'uso di tali risorse e servizi è subordinato al rispetto da parte degli utenti, oltre che del presente Regolamento, anche delle norme che regolano la Rete Italiana dell'Università e della Ricerca, denominata comunemente "Rete GARR" di cui la rete d'Ateneo è parte.

La rete di Ateneo è unica ed unitaria. La gestione della Rete è delegata al Centro di ateneo per i Servizi Informativi, in seguito indicato come C.S.I.

Art. 2: Finalità dell'utilizzazione della Rete di Ateneo

La Rete è utilizzata a supporto delle attività didattiche, di ricerca, di terza missione, tecniche, amministrative e, in generale, di tutte le attività istituzionali dell'Università, nonché come strumento utile alla comunità di Ateneo.

È vietato utilizzare la Rete per scopi incompatibili con quelli stabiliti dal presente Regolamento e in violazione di leggi penali, civili ed amministrative.

Art. 3: Gestione della Rete di Ateneo

Il C.S.I. è delegato alla gestione dell'infrastruttura fisica - apparati attivi di rete, cablaggi utilizzati per la connessione degli utenti contenuti negli armadi di rete - e di quella logica - configurazione degli accessi e dei protocolli attivi, monitoraggio del corretto utilizzo e funzionamento.

Il C.S.I. individua il responsabile della Rete mediante Decreto del Presidente.

Il responsabile della Rete ha il compito di monitorare, coordinare e gestire tutte le problematiche tecniche relative alla Rete.

Le strutture decentrate dell'Ateneo individuano al loro interno un referente informatico di struttura che, seguendo le indicazioni del responsabile della Rete, gestisce gli accessi relativi alla struttura di appartenenza.

Art. 4: Utenti della Rete di Ateneo

Hanno diritto di accedere alla Rete, secondo le modalità di seguito definite e limitatamente al periodo in cui intercorre il rapporto con l'Università degli Studi di Napoli Federico II:

a. il personale docente, i ricercatori, i docenti a contratto, i dottorandi, i titolari di borse post-dottorato, i titolari di borse, assegni o contratti di ricerca;
b. il personale tecnico-amministrativo, compreso il personale a tempo determinato ed i titolari di contratti di collaborazione;
c. i componenti degli organi di governo;
d. gli studenti.

L'accesso è inoltre consentito, previa autorizzazione e limitatamente allo svolgimento delle relative attività,

e. ai partecipanti ed i relatori di convegni/seminari gestiti o organizzati dall'Università anche in compartecipazione con altri enti;
f. ai collaboratori e i ricercatori esterni impegnati in attività da svolgersi all'interno dell'Università;
g. ai consulenti ed i dipendenti e collaboratori di società fornitrici i quali abbiano necessità di accedere alla Rete di Ateneo per lo svolgimento delle attività di cui sono stati incaricati per tutto il tempo della durata dell'appalto;
h. al personale di Enti pubblici o privati secondo quanto previsto all'Art. 9.

Art. 5: Modalità di accesso alla Rete di Ateneo

Esistono diverse modalità di accesso alla Rete di Ateneo:

1- **tramite collegamento wired**, cioè con l'uso di apparecchiature informatiche collegate tramite il sistema di cablaggio passivo della struttura, ad uno apparato di rete (switch) che è a sua volta connesso alla Rete, direttamente o indirettamente. Le apparecchiature collegabili in rete wired sono: PC fisso o portatile, server, sistemi di storage, stampanti o altro tipo di dispositivo dotato di interfaccia di rete wired, come ad esempio strumentazione di laboratorio. L'apparecchiatura connessa può essere di proprietà dell'Ateneo o di altri Enti che operano nelle sedi fisiche dell'Ateneo mediante Convenzioni, e può essere ad uso personale o ad uso collettivo (es. PC dei laboratori). Ogni device collegata wired sarà identificata da un indirizzo IP.

2- **tramite collegamento wireless** attraverso gli Access Point distribuiti all'interno dell'Ateneo, a seguito di autenticazione con le proprie credenziali istituzionali alle reti "Wi-Fi_UniNA" ed "Eduroam". Le apparecchiature collegabili in rete wireless sono Notebook, Tablet, Smartphone, o altro tipo di dispositivo dotato di interfaccia di rete wireless, come ad esempio strumentazione di laboratorio. In specifici casi, l'accesso alla rete wireless può essere reso disponibile anche attraverso modalità diverse previste per gli utenti che non sono titolari credenziali istituzionali, come ad es. in occasione di convegni o conferenze, a seguito di richieste fatte al Responsabile della Rete.

3- **tramite collegamento VPN** (Virtual Private Network) al servizio di accesso remoto a seguito di autenticazione attraverso le credenziali istituzionali o credenziali create ad hoc. L'accesso remoto alla rete d'Ateneo è consentito per esigenze di ricerca, didattica, di servizio, di aggiornamento dei sistemi, di manutenzione delle apparecchiature ed altre attività ad esse riconducibili.

La navigazione, i contenuti visionati e le attività svolte durante l'utilizzo della Rete Telematica di Ateneo restano sotto la totale responsabilità del titolare dell'indirizzo IP nel caso di collegamento wired e del titolare delle credenziali istituzionali nel caso di collegamento wireless.

La cessione delle proprie credenziali istituzionali a terzi è vietata e, comunque, non sottrae il titolare delle credenziali dalla responsabilità conseguenti alle attività svolte utilizzando tali credenziali, secondo quanto riportato nei regolamenti di Ateneo "Utilizzo del servizio di Posta elettronica @studenti.unina.it" e "Utilizzo del servizio di Posta elettronica @unina.it".

Alla gestione della Rete sono legati dei sistemi di tracking e registrazione dei log di navigazione. I log in oggetto saranno conservati secondo quanto specificato dalla normativa vigente e saranno resi disponibili alle autorità giudiziarie in caso di richiesta.

Il servizio è anche dotato di sistema di filtraggio dei contenuti per cui, sia per fini di sicurezza che per evitare un inutile dispendio della banda condivisa agli utenti, in particolari situazioni potrà essere bloccato o limitato un determinato tipo di traffico.

Art. 6: Configurazione dei sistemi connessi alla rete

Possono essere connesse alla rete di Ateneo, direttamente o indirettamente, dispositivi come computer individuali, fissi o portatili e apparecchiature simili, previo rispetto di regole di sicurezza.

La connessione di questo tipo richiede la configurazione di alcuni parametri, che vengono assegnate in due modalità:

i) **in modo statico** con indirizzi IP pubblici (a cura del referente informatico di struttura o suo delegato e/o del personale del C.S.I): gli indirizzi IP delle postazioni e delle apparecchiature e la relativa maschera di sottorete, dovranno essere esclusivamente appartenere a quelli assegnati dal C.S.I. alla struttura; il DNS (primario e secondario) dovrà essere indicato in base a quanto disposto dal C.S.I. (192.133.28.1 e 192.133.28.7 rispettivamente); è esplicitamente vietato l'uso di indirizzi "non UNINA" come DNS.

ii) **in modo dinamico** (tramite il protocollo DHCP): gli indirizzi potranno essere individuati con indirizzi pubblici come nel caso *i)*, ma con assegnazione prefissata in base all'indirizzo fisico della postazione o dell'attrezzatura, oppure potranno essere assegnati dinamicamente come indirizzi privati; in questo caso attraverso il protocollo NAT (Network Address Translation) sarà comunque possibile accedere alla rete Internet. Vale la stessa regola del caso *i)* per quanto riguarda il DNS.

Per quanto riguarda le stampanti, ad esse andrà inibito l'accesso da e verso ogni rete diversa dalla rete locale della struttura, mediante opportune configurazioni che saranno dettate dal referente informatico di struttura, sentito il responsabile della Rete.

Per quanto riguarda i server ed i Network Attached Storage, essi andranno configurati con indirizzi pubblici solo se strettamente necessario alle attività didattiche e di ricerca della struttura e/o del gruppo di ricerca e/o del docente o ricercatore. La lista di questi apparati, con le loro caratteristiche software e gli indirizzi assegnati, andrà comunicata al Responsabile della Rete, ed i dati andranno aggiornati ad ogni modifica.

Non è consentito l'accesso a questi dispositivi per il tramite di modem, inclusi quelli 4G/5G, o altre modalità che consentano l'accesso diretto alle apparecchiature senza passare per gli apparati centrali della rete di Ateneo.

Il personale del C.S.I., su richiesta del Responsabile della Rete, potrà effettuare verifiche e richiedere modifiche alle configurazioni, ove ricorrano condizioni che inficiano la sicurezza della rete di Ateneo.

Art. 7: Accesso remoto

Il C.S.I. rende disponibile, in funzione delle esigenze, due modalità di accesso remoto:

1. accesso tramite collegamento VPN:
è il servizio di accesso remoto autenticato (attraverso le credenziali istituzionali o credenziali create ad hoc) tramite VPN (Virtual Private Network) per accedere dall'esterno alla rete d'Ateneo per esigenze di ricerca, didattica, di servizio, di aggiornamento dei sistemi, di manutenzione delle apparecchiature ed attività ad esse riconducibili.
L'utilizzo di programmi di desktop remoto o condivisione di risorse (VNC, TeamViewer, ecc.), o altri collegamenti creati adhoc saranno consentiti solo a valle della creazione di un collegamento VPN. Non è consentito l'accesso tramite *backdoor* di qualsiasi tipo (openVPN o similari), ovvero evitando il controllo di accesso fatto dai sistemi centrali di rete del C.S.I..

2. accesso tramite Proxy:
è il servizio attraverso il quale gli utenti in possesso delle credenziali istituzionali possono, una volta autenticati, accedere alle risorse digitali ed alle banche dati acquisite dall'Ateneo. Utilizzi del Proxy per usi diversi da quelli istituzionali non sono consentiti e potranno essere inibiti.

I log dei collegamenti remoti saranno mantenuti per un massimo di 12 mesi, senza che il personale del C.S.I. vi possa accedere se non statisticamente, e gli stessi saranno resi disponibili all'autorità giudiziaria in caso di richiesta esplicita e scritta.

Il Responsabile della Rete di Ateneo, previa autorizzazione del Presidente del C.S.I., potrà interrompere in qualsiasi momento, per motivi di sicurezza, il servizio di accesso remoto, laddove si manifestino situazioni di palese pericolo o compromissione della rete.

Art. 8: Violazioni

Le violazioni delle disposizioni del presente Regolamento da parte del personale docente, ricercatore, tecnico amministrativo e da parte degli studenti, costituiscono violazioni degli obblighi di comportamento e sono valutate quali eventuali ipotesi di responsabilità disciplinare secondo i principi e le modalità previste dagli specifici codici di disciplina.
Delle intervenute violazioni sarà altresì presentata denuncia alle Autorità competenti ove appaiano configurarsi ipotesi di responsabilità civile, penale o amministrativa.

Art. 9: Interazione con altri soggetti

L'Ateneo, in base ad espliciti protocolli, convenzioni ed altre forme di collaborazione, consente l'accesso alla propria rete ad enti esterni, come AOU, INFN, CNR, Accademie, Scarl etc. che operano all'interno delle sedi dell'Ateneo stesso. Le specifiche esigenze di questi enti, in merito all'accesso alla rete, saranno oggetto di accordi scritte come le Convenzioni Attuative previste negli Accordi Quadro, o altre forme di contrattualizzazione, che terranno conto delle specifiche esigenze di questi enti ai fini della ricerca e della didattica.