U.S.R.

IL RETTORE

VISTO lo Statuto di Ateneo;

VISTO il D.Lgs. 7 marzo 2005, n. 82 e ss.mm.ii., recante il *"Codice dell'Amministrazione Digitale"*;

VISTO il *Regolamento sull'accesso e l'utilizzazione della rete informatica e telematica di Ateneo*, emanato con D.R. n. 4754 del 22/11/2019;

VISTA la Nota PG n. 76239 del 18/06/2024 con la quale il *Centro di Servizio di Ateneo per i Servizi Informativi (CSI)* ha proposto modifiche del suddetto Regolamento al fine di adeguane le previsioni in relazione all'intervenuto ammodernamento delle infrastrutture della rete informatica e telematica dell'Ateneo ed all'esigenza di rafforzare le azioni da adottare nell'ambito delle politiche di cybersecurity volte a garantire la sicurezza dei sistemi informatici e telematici;

VISTA la Delibera n. 31 del 02/10/2024 (EO n. 1047 del 09/10/2024) con la quale il Senato Accademico ha approvato, subordinatamente al parere favorevole del Consiglio di Amministrazione, le sopra accennate modifiche del *Regolamento sull'accesso e l'utilizzazione della rete informatica e telematica di Ateneo,* nel testo proposto dal Centro di Servizio di Ateneo per i Servizi Informativi (CSI) con la sopra citata nota PG n 76239 del 18/06/2024;

VISTA la Delibera n.149 del 02/10/2024 (EO n. 1084 dell'11/10/2024) con la quale il Consiglio di Amministrazione ha espresso parere favorevole in merito alle suddette modifiche del *Regolamento sull'accesso e l'utilizzazione della rete informatica e telematica di Ateneo;*

DECRETA

Il *Regolamento sull'accesso e l'utilizzazione della rete informatica e telematica di Ateneo* è modificato come da stesura allegata quale parte integrante e sostanziale del presente Decreto.

Il suddetto Regolamento modificato entra in vigore il giorno successivo a quello della sua pubblicazione all'Albo Ufficiale dell'Ateneo e, da quella data, sostituisce il Regolamento emanato con il D.R. n. 4754/2019, citato in premessa.

IL RETTORE
Matteo LORITO

Area Affari Generali e Gestione Documentale
Il Dirigente: *dott. Francesco BELLO*
Unità organizzativa responsabile del procedimento:
Ufficio Statuto, Regolamenti e Organi Universitari
Responsabile del Procedimento:
Il Capo dell'Ufficio: *dott. Antonio NASTI*

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
DR/2024/5243 del 25/11/2024
Firmatari: LORITO Matteo

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 CSI è il Centro delegato alla gestione dell'infrastruttura fisica (intesa come apparati attivi di rete e cablaggio strutturato utilizzato per la connessione degli utenti) e di quella logica (intesa come la configurazione degli accessi e dei protocolli attivi, il monitoraggio del corretto utilizzo dell'infrastruttura ed il suo funzionamento operativo).

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024

Su proposta del Presidente del CSI, con Decreto del Direttore Generale, è individuato tra i Direttori Tecnici della Divisione Networking del CSI il Responsabile della Rete di Ateneo.

Le Strutture decentrate dell'Ateneo individuano al loro interno un Referente Informatico di Struttura che, seguendo le indicazioni del Responsabile della Rete di Ateneo, gestisce gli accessi relativi alla struttura di appartenenza.

Il Responsabile della Rete di Ateneo, coadiuvato dal personale delle Aree del CSI afferenti alla Divisione Networking e dai Referenti Informatici di Struttura, ha il compito di monitorare, coordinare e gestire tutte le problematiche tecniche relative alla Rete e alla Sicurezza Informatica della stessa, adottando tutte le misure atte ad assicurare usi leciti della rete.

Il Responsabile della Rete di Ateneo si occupa di:

- Sviluppare, documentare e diffondere le Politiche di Sicurezza delle Informazioni;
- Formare ed aggiornare i Referenti Informatici di Struttura su questioni di sicurezza della Rete di Ateneo;
- Comunicare informazioni riguardanti le politiche di Cybersecurity, traducendole in regole di Sicurezza da implementare sui sistemi di gestione della Rete di Ateneo;

Al personale della Divisione Networking, inoltre, è rimesso lo svolgimento delle seguenti attività:

- monitorare le comunicazioni e i dati che utilizzano la Rete o i Sistemi dell'Università;
- condurre scansioni di vulnerabilità di qualsiasi Risorsa Informatica collegata alla Rete dell'Università;
- disconnettere dalla Rete di Ateneo le apparecchiature informatiche (router, access-point, switch/hub, NAS, e similari) che presentano un rischio per la sicurezza dalla Rete dell'Università;
- conservare i log di rete su appositi sistemi di "logging" per un minimo di 6 mesi;
- collaborare e supportare la Polizia Postale e le Autorità competenti in caso di uso illecito delle risorse informatiche.

I Referenti Informatici di Struttura, scelti tra il personale universitario afferente alla Struttura, vengono nominati dal Direttore della Struttura e hanno il compito di:

- mantenere un inventario di tutti gli Endpoint utilizzati nelle rispettive aree di responsabilità;
- condurre controlli periodici della sicurezza dei Sistemi e delle Reti, nelle rispettive aree di responsabilità;
- gestire localmente l'indirizzamento IP degli endpoint e di tutti i sistemi informatici presenti nelle rispettive aree di responsabilità.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024

Art. 4: Utenti della Rete di Ateneo

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

1. 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;
2. il personale tecnico-amministrativo e bibliotecario, compreso il personale a tempo determinato ed i titolari di contratti di collaborazione;
3. i componenti degli organi di governo;
4. gli studenti.

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

5. ai partecipanti ed ai relatori di convegni/seminari gestiti o organizzati dall'Università anche in compartecipazione con altri enti;
6. ai collaboratori ed ai ricercatori esterni impegnati in attività da svolgersi all'interno dell'Università;
7. ai consulenti ed ai 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 l'intera durata dell'appalto;
8. al personale di Enti pubblici o privati e di società che operano attraverso appositi contratti o convenzioni all'interno dell'Ateno. In particolare, 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, ecc.) 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 scritti, 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.

In generale, si definiscono "Utenti" tutte le persone che utilizzano la Rete di Ateneo. Gli Utenti sono responsabili di garantire che le risorse dell'Ateneo siano utilizzate correttamente, in conformità con il Regolamento di accesso alla rete della Federico II e che le credenziali, o, in generale, le informazioni personali, non siano rese disponibili a persone non autorizzate.

Risulta invece, categoricamente vietato utilizzare la Rete per scopi incompatibili con quelli stabiliti dal presente Regolamento e in violazione alle leggi penali, civili ed amministrative dello Stato italiano.

In particolare, nessun Utente può intraprendere nessuna delle seguenti azioni:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024

- utilizzare la Rete di Ateneo in violazione delle Politiche di Sicurezza delle Informazioni;
- violare qualsiasi politica o procedura istituzionale o utilizzare la Rete di Ateneo per scopi non etici, illegali o criminali;
- copiare, distribuire o trasmettere materiali protetti da copyright, in assenza di opportuna autorizzazione;
- ostacolare il lavoro dell'Università, consumando quantità eccessive di banda della Rete o di altre risorse e sistemi dell'Ateneo;
- intimidire, molestare, minacciare o comunque danneggiare altri Utenti o Risorse Informative interne o esterne, compresi, ma non limitati a: Diffamazione, Cyberbullismo, Deep fake, Cyberstalking, uso non consensuale di immagini, acquisizione di identità digitali altrui;
- causare intenzionalmente un incidente di sicurezza (ad esempio, accedere a un account o a Dati dell'Università cui l'Utente non è autorizzato ad accedere, ecc.);
- eludere l'autenticazione dell'Utente o la sicurezza dei Sistemi o dei Terminali;
- creare o rilasciare intenzionalmente virus informatici o worm, o compromettere in altro modo un computer;
- utilizzare la Rete Universitaria per ottenere accesso non autorizzato a un Sistema o ai Dati dell'Università o per aumentare i privilegi su un Sistema;
- utilizzare la Rete di Ateneo per scopi commerciali o politici, tranne quando esplicitamente approvato dalla Governance dell'Ateneo.

Allo stesso tempo, ciascun Utente deve intraprendere le seguenti azioni:

- assicurarsi che il proprio account o password siano utilizzati correttamente e non vengano trasferiti o utilizzati da un'altra persona;
- disconnettersi dai sistemi di Ateneo e dalla propria postazione dopo aver completato il proprio turno di lavoro o quando si lascia incustodita la postazione di lavoro;
- segnalare la perdita o il furto di qualsiasi Endpoint o Sistema contenente Dati Sensibili con cui è possibile risalire a dati o credenziali relative all'Ateneo;
- utilizzare i Sistemi Email dell'Università solo in conformità a quanto stabilito dalle leggi e dai regolamenti.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024

Art. 5: Modalità di accesso alla Rete di Ateneo

Esistono diverse modalità di accesso alla Rete di Ateneo:

- Wired: attraverso la rete cablata;
- Wireless: attraverso il collegamento agli Access Point distribuiti all'interno dell'Ateneo;
- Remoto: attraverso collegamento VPN (Virtual Private Network).

Modalità di accesso alla Rete Wired

Il collegamento wired, avviene collegando il dispositivo alla presa di rete dati disponibile, attraverso un cavo in rame (bretella o patch cord). Tramite il sistema di cablaggio passivo orizzontale, le apparecchiature informatiche vengono collegate quindi ad un apparato di rete (switch), che è a sua volta connesso direttamente alla Rete Telematica.

Le apparecchiature collegabili in rete wired sono: computer fisso o portatile, server, sistemi di storage, strumentazione di laboratorio, stampanti o altro tipo di dispositivo dotato di interfaccia di rete wired. 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 dispositivo collegato alla rete wired di Ateneo sarà identificato da un indirizzo IP.

Si sottolineano i seguenti punti di fondamentale importanza:

- risulta vietato, al fine di non permettere accessi non autorizzati alla Rete di Ateneo, attestare sulla rete wired router, switch o altre apparecchiature che consentano di mascherare o evitare il riconoscimento degli host: ogni dispositivo che si attesta sulla rete di ateneo dovrà essere autorizzato, identificato e catalogato in maniera univoca;
- se una struttura, in maniera autonoma, decide di approvvigionarsi, a proprie spese, di specifici apparati di rete, i nuovi apparati possono essere acquistati dopo aver ricevuto l'autorizzazione del CSI. Tali apparati dovranno essere compatibili con la rete di Ateneo e la loro gestione sarà comunque operata dalla Divisione Networking che ne uniformerà la configurazione di utilizzo;
- tutti i device di rete, quali Telecamere, Nas e similari, prima di essere immessi sulla rete di Ateneo dovranno essere autorizzati dal CSI, essere catalogati e ben configurati, in maniera da non essere visibili da rete pubblica. Gli indirizzi di rete impiegati dovranno essere di tipo privato, raggiungibili dall'esterno solo attraverso la VPN.
- non è consentito modificare il MAC address del singolo host per eludere eventuali controlli degli accessi basati su tale tipo di filtraggio.

Modalità di accesso alla Rete Wireless

L'accesso alla rete wireless avviene attraverso collegamento agli Access Point distribuiti all'interno dell'Ateneo, dopo aver eseguito l'autenticazione attraverso l'inserimento delle proprie credenziali istituzionali. A quel punto, attraverso la creazione di un canale di comunicazione sicuro, si accede con il proprio dispositivo alla Rete di Ateneo. Su tutti gli AP presenti all'interno dell'Ateneo viene "annunciata" e resa disponibile anche la rete con SSID (Service Set IDentifier) "eduroam" (Education Roaming), che è il servizio che permette agli utenti in mobilità presso altre organizzazioni di accedere in modo semplice e sicuro alla rete wireless usando le credenziali fornite dalla propria organizzazione, che autorizzerà l'accesso alla rete.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024

Le apparecchiature collegabili in rete wireless sono Notebook, Tablet, Smartphone, o altro tipo di dispositivo dotato di interfaccia di rete wireless. Nel caso specifico di apparecchiature quali, ad esempio, strumentazioni di laboratorio che devono essere collegate alla rete ma non permettono una autenticazione tramite credenziali, si possono prevedere accessi di tipo semplificato, ma con un uso della rete che, per ragioni di sicurezza, risulti opportunamente limitato.

In occasione di convegni, conferenze o eventi fruibili all'interno dell'Ateneo, l'accesso alla rete wireless può essere reso disponibile anche attraverso modalità diverse, previste per gli utenti che non sono titolari di credenziali istituzionali. In questi casi, a seguito di specifica richiesta operata attraverso l'apposita modulistica presente sul sito del CSI (www.csi.unina.it), vengono configurati SSID dedicati, che prevedono credenziali con password condivisa. In questo caso, per ragioni di sicurezza informatica, l'accesso alla rete Internet sarà opportunamente limitato.

Per gli utenti "guest", per i quali è prevista una permanenza all'interno dell'Ateneo (partecipanti ad Academy, consulenti o personale esterni), è prevista la creazione di specifici account validi per l'intera durata della permanenza. Parte di questa attività può essere delegata anche ai Referenti Informatici di struttura.

La navigazione, i contenuti visionati e le attività svolte durante l'utilizzo della Rete Telematica di Ateneo restano sotto la totale responsabilità: (i) del titolare dell'indirizzo IP, nel caso di collegamento wired; (ii) 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 dalle responsabilità conseguenti alle attività svolte utilizzando tali credenziali, secondo quanto riportato nei regolamenti specifici di Ateneo quali, ad esempio, quelli sulle politiche di utilizzo della posta elettronica ("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.

Modalità di accesso remoto

Dalla rete Internet, l'accesso alla Rete di Ateneo avviene tramite collegamento VPN (Virtual Private Network). Per l'abilitazione delle credenziali istituzionali (o di credenziali create ad hoc, nel caso di personale esterno), occorre richiedere autorizzazione attraverso apposita modulistica presente sul sito del CSI (www.csi.unina.it). La connessione avviene

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024

attraverso l'utilizzo di client VPN, tramite il quale sarà creato un collegamento crittografato tra il dispositivo utente e la Rete di Ateneo.

L'accesso remoto alla rete d'Ateneo è consentito per esigenze di ricerca, didattica, di servizio, di aggiornamento dei sistemi, di manutenzione delle apparecchiature, nonché per la conduzione di altre attività ad esse riconducibili.

L'utilizzo di programmi di desktop remoto o condivisione di risorse (VNC, TeamViewer, ecc.), o altri collegamenti creati ad hoc 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..

In linea con le normative sulla privacy e sulla sicurezza informatica, i collegamenti remoti di accesso alla rete di Ateneo attraverso client VPN saranno autorizzati attraverso una autenticazione a più fattori (MFA). In particolare, oltre alla classica coppia Username/Password, occorrerà introdurre il secondo fattore di autenticazione attraverso:

- Microsoft Authenticator per gli utenti interni (@unina, @studenti)
- Specifico token distribuito in maniera puntuale per gli utenti esterni.

Un ulteriore servizio offerto dall'Ateneo è quello di accesso tramite Proxy, con cui gli utenti in possesso delle credenziali istituzionali possono, una volta autenticati, accedere alle risorse digitali ed alle banche dati acquisite dall'Ateneo. L'utilizzo del Proxy per usi diversi da quelli istituzionali non è consentito e potrà essere inibito.

I log dei collegamenti remoti saranno mantenuti per un tempo minimo di 6 mesi, senza che il personale del C.S.I. vi possa accedere, se non per l'elaborazione di informazioni aggregate di tipo statistico, in accordo con la normativa vigente in materia di privacy. I log 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. 6: Configurazione dei sistemi connessi alla rete

Possono essere connessi alla rete di Ateneo, direttamente o indirettamente, dispositivi come computer individuali, fissi o portatili e apparecchiature simili, previo rispetto e accettazione delle regole di sicurezza e del presente regolamento di accesso alla rete.

La connessione alla Rete di Ateneo richiede la configurazione di alcuni parametri, che vengono assegnati in due modalità alternative:

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024

1. in modalità statica:
    a. gli indirizzi IP delle postazioni e delle apparecchiature e la relativa maschera di sottorete e gateway dovranno necessariamente appartenere ai lotti di indirizzi assegnati dal C.S.I. alla struttura. Gli indirizzi IP saranno richiesti, in numero adeguato alle esigenze della struttura, dal Direttore di struttura, attraverso apposita modulistica presente sul sito del CSI (www.csi.unina.it). Il CSI assegnerà alla struttura i lotti di indirizzi richiesti, delegando ad essa la distribuzione dei singoli indirizzi. Il Referente Informatico di Struttura si occuperà di annotare le assegnazioni così avvenute.
    b. il DNS (primario e secondario) dovrà essere indicato in base a quanto disposto dal C.S.I. È esplicitamente vietato utilizzare DNS esterni alla rete dell'Università.
2. in modalità dinamica, attraverso il protocollo DHCP:
    a. gli indirizzi e i server DNS saranno assegnati dinamicamente e saranno applicate opportune politiche di "reservation" per garantire una associazione costante tra indirizzo IP assegnato al dispositivo e indirizzo MAC dello stesso.

Gli indirizzi IP distribuiti alle varie strutture saranno di tipo privato, in maniera da non essere direttamente visibili da Internet. In questo caso, attraverso meccanismi di NAT (Network Address Translation), gli indirizzi privati, prima che i pacchetti escano dalla Rete di Ateneo, subiranno un processo di "traduzione" in indirizzi pubblici, per consentire un accesso trasparente alla rete Internet.

Per le strutture a cui in passato sono stati distribuiti indirizzi IP pubblici, il CSI si occuperà di implementare un piano di aggiornamento alla summenzionata politica di indirizzamento privato.

Nel caso di particolari esigenze, la Struttura potrà richiedere la assegnazione di un numero limitato di indirizzi pubblici che saranno, sotto specifica assunzione di responsabilità, rilasciati per fini istituzionali (ad esempio sito dipartimentale o pubblicazioni di risorse on-line).

Il C.S.I. potrà effettuare verifiche di funzionamento, nonché operare attività di "risk assessment" periodiche, al fine di migliorare la resilienza dell'infrastruttura di rete nei confronti di potenziali attacchi informatici. In funzione del risultato di tali attività, il C.S.I. potrà richiedere che siano implementate modifiche alle configurazioni, specialmente nei casi ove ricorrano condizioni che possano inficiare la sicurezza della rete di Ateneo.

Per quanto riguarda stampanti, telecamere e dispositivi di rete non gestiti direttamente dal C.S.I., ad essi 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 dispositivi NAS (Network Attached Storage), essi andranno configurati con indirizzi IP 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

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024

che ne è responsabile. La lista di questi apparati, con le loro caratteristiche software e gli indirizzi assegnati, gestita dal Referente Informatico di Struttura, andrà comunicata al Responsabile della Rete. Tali dati andranno aggiornati ad ogni modifica.

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

Art. 7: Accesso alla rete di Ateneo nel caso di Eventi e Convegni

In occasione di eventi e convegni organizzati nell'ambito dell'Ateneo, il CSI offre vari servizi di accesso alla rete sia wireless che cablata.

Tutte le aule convegni risultano coperte dalla rete Wi-Fi_UniNA ed Eduroam ma, a richiesta, risulta possibile richiedere un SSID dedicato all'evento, per favorire la connettività dei partecipanti non appartenenti ne all'Ateneo ne agli enti di ricerca europei. La richiesta deve essere operata, **almeno tre giorni prima dell'evento**, compilando la specifica modulistica reperibile sul sito del CSI (www.csi.unina.it). A fronte della compilazione della modulistica, sarà configurata una rete wireless dedicata all'evento (il SSID sarà coerente con il "titolo" dell'evento) il cui accesso sarà, generalmente a chiave condivisa. L'accesso a questo tipo di rete wireless assicura l'accesso ad Internet in maniera limitata ai protocolli di uso comune (http, https, posta, etc.).

Risulta possibile, ove presente, connettersi anche alla rete cablata. I punti rete presenti sono telegestiti e rilasceranno indirizzi privati in maniera dinamica che permettono di accedere alla intranet. Per attività di tipo diverso, quali video comunicazioni, streaming o attività che prevedono l'accesso ad Internet, occorrerà compilare specifica modulistica reperibile sul sito del CSI (www.csi.unina.it) indicando il tipo di uso.

Non sarà permesso l'accesso alla rete in maniera non autorizzata dal CSI.

Art. 8: Rilevazione delle minacce

Attraverso i sistemi di logging e di analisi del traffico di rete possono essere riconosciute le minacce alla sicurezza informatica dell'Ateneo. Gli indirizzi IP dei device che risultano fonte di malware o il cui comportamento verrà interpretato dai sistemi di monitoraggio come anomalo, saranno identificati, saranno bloccati o posti in quarantena. Le fonti che saranno prese in considerazione sono:

- Segnalazioni da parte del GARR, dal CNAIPIC, di ACN e dai vari SIRT e CERT nazionali;
- Segnalazioni ricevute dalla organizzazione ShadowServer Foundation,

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024

- Sistemi di *threat intelligence*, monitoraggio e SIEM gestiti dal C.S.I..

Gli indirizzi IP oggetto delle segnalazioni, ritenuti pericolosi per la sicurezza informatica, saranno temporaneamente inibiti o limitati nel funzionamento al fine di evitare compromissioni rispetto alla Rete di Ateneo; gli stessi saranno raccolti su un portale, interrogabile solo dall'interno dell'Ateneo, che riporterà le informazioni relative al blocco IP e cosa fare per richiedere lo sblocco.

Art. 9: Violazioni

Le violazioni delle disposizioni del presente Regolamento da parte del personale docente, ricercatore, tecnico amministrativo, nonché 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.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
allegato al DR/2024/5243 del 25/11/2024