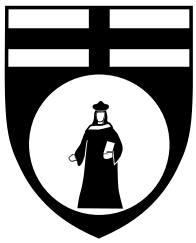

Università
di Genova

Linea Guida ICT

Utilizzo delle reti

Versione	Autori
Ottobre 2024	Agnese Arosio (Area ICT) Giorgio Bertorello (Area ICT) Claudio Di Martino (Area ICT) Francesco Fronda (Area ICT) Massimo Ivaldi (Area ICT) Gianni Verduci (Area ICT) Massimo Di Spigno (Area ICT)

Sommario

Introduzione

L'Università degli Studi di Genova, a cui ci si riferisce in seguito come Unige, o Ateneo, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento deve considerarsi integrato da tutte le procedure interne adottate per argomenti specifici e casistiche, così come pubblicati sul sito dell'Ateneo e più specificatamente dell'Area ICT.

Finalità del documento

Il presente documento è da considerarsi parte integrante delle "Linee guida per la sicurezza e l'utilizzo delle risorse informatiche dell'Ateneo": più specificatamente in questo elaborato si vogliono definire specifiche regole e condizioni di utilizzo della Rete Dati e del Sistema Telefonico di Ateneo.

Contesto normativo e regolamentare

Il presente regolamento è redatto sulla base dei seguenti e principali riferimenti normativi:

- Regolamento dell'Università degli Studi di Genova per la realizzazione e la gestione della rete dati
  https://ict.unige.it/sites/ict.unige.it/files/pagine/Regolamento-reti_0.pdf
- Norme Tecniche Attuative del Regolamento per la realizzazione e la gestione della rete dati
  https://ict.unige.it/sites/ict.unige.it/files/pagine/NormeTecnicheAttuative.pdf
- Acceptable User Policy (AUP) di GARR
  https://www.garr.it/it/regole-di-utilizzo-della-rete-aup

GLOSSARIO E DEFINIZIONI

Ai fini del presente documento si intende per:

- **ACN** https://www.acn.gov.it :
  E' l'Agenzia per la Cybersicurezza Nazionale, istituita dal Decreto-legge n.82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.
  L'Agenzia per la cybersicurezza nazionale (ACN) è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza.
  L'Agenzia ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico. Si occupa di prevenire e mitigare il maggior numero di attacchi cibernetici e di favorire il raggiungimento dell'autonomia tecnologica.

- **AP**
  Acronico di Access Point (Punto di Accesso), identifica l'apparato/dispositivo che eroga le reti wireless GenuaWiFI/Eduroam, diffondendo il segnale radio in un determinato raggio d'azione.

- **AUP** (Acceptable Use Policy) di GARR https://www.garr.it/it/regole-di-utilizzo-della-rete-aup :
  Sono le regole di corretto utilizzo e comportamento emanate dal Consortium GARR, alle quali sono soggetti gli enti autorizzati ad accedere alla Rete GARR.

- **Client**
  In generale, termine che definisce la postazione di lavoro dell'utente. Si tratta del dispositivo terminale, che è interconnesso alla rete dati (sia cabalata che wireless).

- **CSIRT Italia** https://www.csirt.gov.it :
  E'istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN). I compiti del CSIRT sono definiti dal Decreto Legislativo 18 maggio 2018, n. 65 e dal Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 art. 4. Essi includono:
  - il monitoraggio degli incidenti a livello nazionale;
  - l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
  - l'intervento in caso di incidente;
  - l'analisi dinamica dei rischi e degli incidenti;
  - la sensibilizzazione situazionale;
  - la partecipazione alla rete dei CSIRT.

- Il CSIRT stabilisce relazioni di cooperazione con il settore privato.
  Per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e dei rischi e sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

- **Eduroam** (*EDUcation ROAMing*) https://eduroam.org :
  E'il servizio internazionale di roaming wireless per persone che lavorano nella ricerca e nell'istruzione superiore.
  Fornisce a ricercatori, insegnanti e studenti accesso facile e sicuro alla rete quando visitano istituzioni diverse da quella in cui lavorano. L'autenticazione degli utenti è eseguita dalla loro istituzione di origine, usando le stesse credenziali fornite da essa, mentre l'autorizzazione all'accesso a Internet e ad altre risorse è gestita dall'istituzione ospite. Non è richiesto alcun pagamento per l'utilizzo di eduroam. Il servizio è fornito a livello locale dalle istituzioni partecipanti (università, istituti di ricerca ecc.), mentre a livello nazionale è organizzato dagli operatori del paese.

- **GARR** https://www.garr.it :
  E' la rete nazionale ad altissima capacità dedicata alla comunità dell'istruzione, della ricerca e della cultura. Il suo principale obiettivo è quello di fornire connettività ad alte prestazioni e di sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti e per la collaborazione a livello internazionale.
  La rete GARR è progettata e gestita dal Consortium GARR, un'associazione senza fini di lucro fondata sotto l'egida del Ministero dell'Istruzione, dell'Università e della Ricerca. Gli enti soci sono CNR, ENEA, INAF, INGN, INGV e tutte le università italiane rappresentate dalla Fondazione CRUI.

- **GenuaNET**:
  E'il sistema integrato di reti dell'Università degli Studi di Genova ed è composto da:
  - rete geografica: realizza l'interconnessione dei poli genovesi e dei poli distaccati dell'Università di Genova e comprende collegamenti verso l'esterno dell'Ateneo; per poli si intendono edifici o gruppi di edifici nei quali sono dislocate strutture universitarie;
  - reti comprensoriali: all'interno di un polo, realizzano l'interconnessione fra le reti locali e la rete geografica;
  - reti locali: realizzano le interconnessioni interne alle strutture universitarie;
  - rete wireless di Ateneo (GENUAwi-fi)

- **GENUAwi-fi**:
  E'la rete componente GENUAnet realizzata con tecnologia wireless, gestita in modo centralizzato e utilizzabile da coloro che dispongono delle credenziali personali UniGePASS; complementa la rete cablata (wired);

- **Indirizzo IP**
  E' una sequenza numerica, che identifica una interfaccia di rete, connessa ad una rete che implementa i protocolli TCP/IP.

- **Indirizzo IP privato**
  Identifica una interfaccia di rete utilizzando un indirizzamento non raggiungibile direttamente da Internet.

- **Proxy server**
  Server che viene utilizzato come intermediario tra le richieste di un client e il server

finale destinatario delle richieste. È impiegato all'interno di reti complesse con diverse finalità, per migliorare la sicurezza e l'efficienza nell'erogazione dei servizi.

- **UniGePass** https://ict.unige.it/UniGePASS :
  E'il sistema di autenticazione di Ateneo, che consente agli utenti di accedere alla rete e alla maggior parte dei servizi informatici mediante le credenziali personali UniGePASS, attualmente costituite da nome utente, password ed eventuale secondo fattore di autenticazione (2FA).

PRINCIPI GENERALI

GenuaNet è la rete telematica dell'Ateneo che ha lo scopo di collegare tutte le aree ove sono ubicate le sedi dedicate alla didattica, alla ricerca e agli uffici amministrativi, distribuite sia in ambito cittadino che in quello regionale. La sua architettura è complessa e comprende sia la rete geografica che quelle di comprensorio, le reti locali e quelle wireless.

Utilizzando la rete GenuaNET e la connessione di GenuaNET a internet tramite la rete GARR, è possibile per i suoi utenti collegarsi alla rete e interagire per gli scopi più diversi, come, per es., la consultazione di archivi e banche dati, la partecipazione a corsi o conferenze on-line, l'utilizzo di risorse computazionali, lo scambio di informazioni, utilizzando sistemi di interconnessione moderni e all'avanguardia.

La complessità, l'estensione e la pervasività della rete pongono inoltre sfide importanti per l'implementazione di adeguati livelli di sicurezza (relativi a riservatezza, integrità e disponibilità) sia della rete stessa che delle risorse accessibili per suo tramite.

L'Area ICT dell'Ateneo ha nel tempo sviluppato, adottato e consolidato strategie al fine di favorire e semplificare le attività di messa in sicurezza della rete stessa, dei servizi erogati in rete, come pure dei dati custoditi sui sistemi ad essa collegati, avvallate anche dalle good practices diventate di implementazione comune.

A titolo esemplificativo (e non esaustivo) indichiamo tra le strategie adottate:

- Azioni per minimizzare la superficie esposta a potenziali attacchi:
    - Conoscere approfonditamente i servizi di rete pubblicati e i sistemi ad essa collegati
    - Evitare l'esposizione non mediata dei servizi e dei sistemi
    - Consentire l'accesso ad ogni specifica risorsa di rete solo alle postazioni/utenze che ne hanno effettiva necessità

- Azioni per ridurre l'impatto di eventuali guasti o malfunzionamenti di componenti HW o SW:
    - Ridondare tutte le componenti HW e SW per non avere singoli punti di fallimento
    - Aggiornare e manutenere accuratamente, puntualmente e costantemente tutte le componenti HW e SW che costituiscono l'infrastruttura dei servizi di rete

- Azioni atte a validare tutti gli accessi in maniera motivata, non per default:
    - Adottare tecniche di autenticazione e autorizzazione all'accesso solide ed efficaci
    - Autorizzare all'accesso sulla base di ruoli e funzioni

- Studio delle minacce più comuni e di quelle emergenti per mantenere un costante ed aggiornato livello di conoscenza e di consapevolezza delle problematiche associate e per una adeguata adozione di misure e strategie di contenimento del rischio ad esse connesse

- Attività di monitoraggio delle risorse nelle reti interne alle Strutture

- Adozione di piani di formazione e aggiornamento di tutti gli utenti

L'applicazione delle strategie sopra elencate e il costante aggiornamento delle azioni di mitigazione dei rischi finora adottate, ha portato l'Area ICT a sviluppare le regole sotto riportate a cui si dovrà fare esplicito riferimento a seconda delle aree di intervento o di interesse.

REGOLE PER L'UTILIZZO DELLA RETE CABLATA

Disposizioni generali

I dispositivi di qualunque natura utilizzati dalle Aree, dai Centri, dalle Scuole, dai Dipartimenti e dal personale e gli utenti relativi, possono essere collegati alla LAN della struttura di appartenenza, rispettando le seguenti norme:

- la Rete può essere usata esclusivamente per le attività istituzionali;
- l'accesso alla Rete di Ateneo dovrà, comunque e in qualsiasi caso, essere conforme alle regole stabilite dall'Ateneo e dalle AUP del GARR;
- la gestione delle interconnessioni comuni ad altri Enti è condotta dall'Area ICT insieme ai rispettivi gestori degli Enti stessi, secondo protocolli definiti da accordi specifici;
- nessuna Struttura può attivare connessioni autonome dalle proprie reti locali di struttura con quelle di altre Strutture, se non concordate ed approvate preventivamente dall'Area ICT;
- per avere un chiaro controllo dei flussi comunicativi, anche internamente ad ogni Struttura deve essere mantenuta una topologia logica e fisica di rete che non presenti interconnessioni che realizzino magliature, di fatto moltiplicando i percorsi possibili;
- ogni Struttura che, a protezione della propria rete locale, abbia necessità di impiegare firewall, è tenuta a comunicare e concordare con l'Area ICT la configurazione degli stessi, prima della relativa implementazione, in modo da poter armonizzare le policy implementate con quelle di Ateneo e delle altre Strutture e assicurare l'accesso ai servizi di Ateneo dalle postazioni locali;
- tutti i sistemi collegati alla rete devono essere identificati, conosciuti e riconducibili ad almeno un referente responsabile che sia contattabile in caso di necessità e ne devono essere registrati gli indirizzi IP assegnati, interno alla Struttura oppure di riferimento nel polo territoriale di competenza;
- l'auto assegnazione da parte dell'utente di indirizzi IP è espressamente vietata;
- tutti gli utenti a cui viene fornito accesso alla Rete devono essere identificati e identificabili;
- l'accesso a Internet da postazioni accessibili al pubblico può essere effettuato solo tramite accreditamento con credenziali personali e deve essere trattato a norma di legge.

Inoltre:

- l'accesso alle risorse della rete è personale e non può essere condiviso o ceduto;
- la responsabilità del contenuto dei materiali prodotti e diffusi attraverso la rete è delle persone che li producono e diffondono;
- gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso;
- gli utenti sono responsabili delle attività svolte sui dispositivi che possano compromettere la piena funzionalità e sicurezza della rete e dei sistemi ad essa collegati.

Regole per l'implementazione della Rete Cablata: segmentazione

Al fine di rispettare i criteri generali sopra indicati, come regola tecnica principe da seguire nell'implementazione di reti cablate si richiede di effettuare la cosiddetta "segmentazione" (possibilmente fisica) della rete, prevedendo l'assegnazione di indirizzi privati in segmenti di rete classificati.

In particolare, si raccomanda di prevedere almeno:

- un segmento ben identificato e destinato ai dispositivi classificati "insicuri" (guest, non amministrati direttamente, non rispondente agli standard di sicurezza individuati, ecc.);
- un segmento destinato ai dispositivi approvati e quindi indicato come "sicuro";
- una serie di sottoreti opportunamente suddivise, isolate e protette riservate ai servizi erogati.

La corretta classificazione dei segmenti di rete consente una gestione più semplice, ordinata e coordinata delle regole che determinano i flussi di comunicazione validati e ammessi all'interno della rete GenuaNET e verso internet.

Nel rispetto della suddetta classificazione, sarà quindi possibile collegare un dispositivo in rete, attraverso apposite prese allestite nei locali, purché, per le Scuole, i Dipartimenti e i Centri, venga richiesto preventivamente all'Area ICT, attraverso richiesta al Presidio Territoriale di competenza, la verifica preventiva della fattibilità, interfacciandosi con il Settore Rete Dati e Fonia, attraverso il canale messo a disposizione dall'indirizzo e-mail di servizio retifonia@unige.it .

È altresì possibile utilizzare la rete cablata per collegare PC personali, purché vengano rispettati i requisiti di sicurezza forniti dall'Area ICT e la collocazione nei segmenti di rete classificati a tal scopo.

Per tale motivo è necessario, per i Dipartimenti e i Centri, fare riferimento alle indicazioni dei propri referenti ICT, che potranno interfacciarsi con i Presidi di Facility Management, e per l'Amministrazione Centrale e i Servizi Tecnici, fare riferimento diretto ai Presidi stessi.

Se le caratteristiche dei dispositivi saranno tali da rispettare i requisiti di sicurezza indicati, sia dal punto di vista software che hardware, la postazione potrà essere considerata idonea per la configurazione in rete che prevederà in ogni caso l'assegnazione di un indirizzo IP privato e l'impiego del proxy server per il controllo del traffico.

Procedure per la realizzazione ex novo/rinnovo/ della Rete Cablata

In caso non fossero presenti prese di rete in numero sufficiente nei locali in cui è richiesto l'utilizzo, è necessario attenersi alle seguenti indicazioni:

1. in caso di progettazione di nuovi edifici e nelle ristrutturazioni di edifici o di porzioni di essi l'Ateneo prevede, finanzia e realizza tramite l'Area ICT la connessione in rete locale di ogni postazione telematica di lavoro o di studio (cablaggio standard) di ciascuna Struttura, comprese le apparecchiature di rete: l'Area ICT provvede, pertanto, a realizzare il cablaggio "verticale" di dorsale a proprio carico, fornendo connettività ai piani degli edifici;

2. in caso di impianti esistenti, ma non più a norma oppure obsoleti e nel caso in cui una rete locale di Struttura risulti non più adeguata alle necessità della Struttura stessa

- i Centri, le Scuole e i Dipartimenti possono estendere il cablaggio "orizzontale" in completa autonomia, a proprio carico, purché la modalità sia compatibile con le caratteristiche dell'infrastruttura di rete; in questo caso, le Strutture che intendono procedere a nuove realizzazioni o a modifiche delle proprie reti locali sono tenute a presentare preventivamente all'Area ICT il progetto, redatto da un professionista abilitato, delle opere che intendono realizzare, fornendo le caratteristiche degli apparati e l'opportuna documentazione aggiuntiva, completa delle specifiche metriche dell'impianto;

su richiesta della Struttura o su proposta dell'Area ICT, il rifacimento e/o l'aggiornamento del cablaggio può essere realizzato a cura e spese dell'Ateneo attraverso l'Area ICT, nel rispetto della propria pianificazione e programmazione temporale oppure a cura e spese della Struttura, con le modalità sopra descritte. Potrà essere prevista una suddivisione della spesa. Gli interventi sono effettuati rispettando le seguenti modalità:

a) la Struttura che intende richiedere all'Amministrazione l'esecuzione di opere di cui al punto 2, deve inviare una circostanziata richiesta indirizzata al Pro-Rettore per gli aspetti informatici;
b) le priorità degli interventi sono definite dal Pro-Rettore per gli aspetti informatici, sentita la Commissione ICT;
c) gli aggiornamenti o ampliamenti devono tenere conto dello stato dell'arte della tecnologia delle reti;
d) l'Ateneo assegna annualmente all'Area ICT, che ne potrà disporre con piena autonomia, uno specifico budget per piccoli interventi di estrema urgenza;
e) gli interventi di manutenzione straordinaria e le nuove esecuzione di non modesta entità, devono essere pianificati e programmati in sede di bilancio di previsione (periodo settembre – dicembre);
f) rispetto ai progetti presentati dalle Strutture, l'Area ICT fornisce un parere tecnico scritto vincolante, indicando anche l'eventuale partecipazione finanziaria da parte dell'Ateneo;
g) la Struttura può anticipare la quota di finanziamento di competenza del Bilancio Universitario, previa approvazione scritta di quest'ultima, oppure sostenere interamente la spesa a titolo definitivo;
h) ai fini dell'ammissibilità del progetto, gli apparati di rete da installare a cura delle Strutture devono essere conformi agli standard di gestione remota ed accessibili in remoto, in caso di necessità, anche dai tecnici dell'Area ICT.
i) al termine di ogni modifica di una rete locale di struttura, il Responsabile della Struttura deve consegnare all'Area ICT copia della documentazione comprensiva di:

- certificazione del cablaggio in base alla normativa nazionale ed internazionale vigente;
- parametri di configurazione degli apparati installati;
- eventuali password non privilegiate delle apparecchiature di rete installate, che permettano il monitoraggio in caso di problemi ed emergenze;
- pianta aggiornata che riporti la topologia fisica e logica della rete locale della struttura.

  In assenza di suddetti elementi, l'Area ICT non configurerà, nei nodi delle dorsali di rete di Ateneo, alcuna connessione con gli apparati di rete della Struttura oggetto della modifica; la rete di struttura rimarrà quindi non connessa alla rete di Ateneo;

j) nel caso in cui l'impianto in oggetto risultasse già collegato alla rete di Ateneo, pur non avendone i requisiti, l'Area ICT non fornirà alcun tipo di supporto e si riserva la facoltà di disconnettere la porzione d'impianto, eventualmente anche senza preavviso, in caso essa possa pregiudicare il funzionamento o la sicurezza della rete Genuanet;
k) la gestione dell'infrastruttura di Rete è attribuita alla Struttura finale e sarà da essa condotta avvalendosi dei referenti tecnici informatici della Struttura, funzionalmente dipendenti dall'Area ICT (come da atto organizzativo in vigore dal 1/1/2024), oppure affidando le attività a un manutentore esterno che può intervenire interfacciandosi e concordando le modalità di gestione con l'Area ICT.

Regole per la configurazione delle postazioni di lavoro: client e servizi di rete

Nel sistema di reti di Ateneo viene garantito il supporto della famiglia di protocolli TCP/IP.

L'Area ICT definisce il piano di indirizzamento IP e assegna segmenti di indirizzi IP privati (validi per le comunicazioni interne e utilizzabili per l'accesso internet via gateway/proxy) e segmenti di indirizzi IP pubblici, da utilizzare esclusivamente per la pubblicazione di servizi che devono essere consultabili da internet. In questo caso, sarà necessario presentare un progetto di fattibilità da sottoporre all'Area ICT.

Al fine di favorire e semplificare le attività di messa in sicurezza dei servizi erogati in rete, come pure dei dati custoditi sui sistemi ad essa collegati, nel tempo si sono adottate e consolidate nell'uso alcune strategie, avvallate anche dalle good practices diventate di implementazione comune e finalizzate a minimizzare la superficie esposta a potenziali attacchi.

Per tale ragione, si rende necessario:

- Conoscere approfonditamente i servizi di rete pubblicati e i sistemi ad essi collegati;
- Evitare l'esposizione non mediata dei servizi e dei sistemi;
- Consentire l'accesso alle risorse di rete solo alle postazioni/utenze che ne hanno necessità.

Le postazioni di rete vengono configurate secondo la seguente logica di assegnazione indirizzi IP:

- Indirizzi IP privati: 10.186.0.0/16 utilizzati da tutte le strutture per le postazioni aperte al pubblico (biblioteche, laboratori, ecc.), per le postazioni utilizzate solo per la navigazione su Internet attraverso proxy di Ateneo e che non devono accedere alle applicazioni Intranet, in generale per i segmenti classificati "insicuri" o di "servizio"
- Indirizzi IP privati: 10.187.0.0/16 utilizzati da tutte le strutture, per le postazioni accessibili solo al personale, amministrate secondo i criteri definiti dall'Area ICT e che devono poter accedere alle applicazioni Intranet, in generale solo ai segmenti classificati "sicuri"

È essenziale attribuire i range di indirizzi privati assegnati alla Struttura, sulla base della classificazione e della destinazione d'uso, ad esempio:

- Range 10.187.X.0/24 "sicuro" destinato a uffici amministrativi e macchine fisse dei docenti, a seconda del tipo di utilizzo;

- Range 10.186.Y.0/24 “insicuro” destinato ad uso laboratori e macchine fisse dei docenti a seconda del tipo di utilizzo;
- Range 10.186.Z.0/24 “insicuro” destinato ad aule informatiche;
- Range 10.186.X.0/24 “servizio” destinato a servizi di Struttura (es. terminali controllo accessi, sistema CCTV, ecc....)
- Altre casistiche, da concordare con l’Area ICT, in caso di necessità.

È inoltre raccomandato evitare di configurare sulla stessa rete IP dispositivi con destinazioni d’uso diversi (es. PC amministrativi con PC laboratori/aula).

Le Strutture Fondamentali possono pertanto precedere autonomamente all’attribuzione degli indirizzi ad esse preventivamente assegnati dall’Area ICT, attraverso il proprio referente ICT di Struttura o, in mancanza, del tecnico informatico del Presidio di competenza;

Viene di norma assegnato alle Strutture anche un range limitato di indirizzi IP pubblici 130.251.0.0/16, che deve essere utilizzato esclusivamente per le postazioni che forniscono un servizio diretto e censito verso Internet.
E’ infatti necessario, nel caso di impiego d’indirizzamento pubblico, registrare il tipo di servizio che il client eroga verso l’esterno di Genuanet, comunicandolo all’Area ICT (v. paragrafo “Procedura di registrazione server”).

Regole per la registrazione di Applicazioni e servizi sulla rete

Le applicazioni in rete devono, in qualsiasi ambito, rispettare l'RFC 1855 "Netiquette Guide Lines", l'Acceptable Use Policy della rete GARR ed ogni altra legge, norma o regolamento relativo alla particolare rete utilizzata.
Le strutture sono tenute a comunicare all’Area ICT l'eventuale presenza di server il cui uso non è confinato localmente al segmento di rete di appartenenza e a presentare preventivamente un documento che illustri eventuali servizi on-line che intendono realizzare o modificare, completo delle specifiche relative a protocolli, criteri di accesso e autenticazione. Al contempo dovranno essere indicati i referenti responsabili del mantenimento in sicurezza e gestione dello stesso, da contattare in caso di anomalie riscontrate e/o segnalate. In caso di decadenza o avvicendamento di tali referenti è necessario darne comunicazione tempestiva all’Area ICT
Questa comunicazione consente all’Area ICT di adottare, eventualmente, misure mirate a garantire ai servizi priorità nel ripristino, di assegnare maggiore banda per le comunicazioni, prevedere meccanismi di monitoraggio, protezione e prevenzione, di differenziare le politiche di accesso a e da tali servizi.

Regole Generali Rete Wireless

L’intero Ateneo è coperto dall’infrastruttura di rete wi-fi gestita dall’Area ICT, che eroga i servizi Eduroam e GenuaWiFI.

Le reti wireless per loro natura non sono confinate e localizzate precisamente e rendono più difficile l'individuazione fisica dell'origine del traffico generato, per cui occorre porre particolare attenzione ai criteri con cui esse vengono realizzate affinché si armonizzino nella gestione con le reti cablate

In generale non è ammesso l'utilizzo di dispositivi wireless di tipo indipendente (stand-alone) per estendere la rete cablata autonomamente. Nel caso in cui la Struttura decida di installare un proprio sistema wireless, l'implementazione deve quindi essere di tipo infrastrutturale, garantire standard implementativi di livello almeno pari a quello realizzato per GenuaWIFI e il progetto deve essere validato dall'Area ICT per i rischi e gli eventuali impatti sulla sicurezza della rete GenuaNET nel suo complesso

In questo caso, l'attività è soggetta alle seguenti norme:

• per l'installazione di un access-point wireless è richiesta la presentazione preventiva di un progetto operativo all'Area ICT: il parere favorevole di quest'ultima è vincolante per il collegamento alla Rete;

• il processo di identificazione, autenticazione e accesso, compresa la conservazione a norma di legge dei dati relativi, è a carico della Struttura;

• devono essere rimossi, o adeguatamente riconfigurati a cura della struttura, gli access point non autorizzati o comunque configurati in modo improprio.

In caso contrario, l'Area ICT si riserva la facoltà di disconnettere le porzioni di infrastruttura non conformi a quanto sopra.

Procedura per autorizzazione presenza AP wireless, non appartenenti all'infrastruttura dell'Area ICT, nelle sedi dell'Università di Genova

Il Decreto del 16 agosto 2005 (G.U. N.190 del 17/8/2005) richiede all'Università di consentire l'uso delle reti wireless a dipendenti, studenti e coloro che in modo occasionale possono utilizzare la connessione ad Internet solo previa autenticazione con credenziali personali. La connessione, attraverso un qualsiasi media trasmissivo di un access point wireless, alla Rete costituisce un ampliamento della rete informatica che sottostà al presente regolamento. È pertanto necessario che la struttura interessata all'attivazione o al mantenimento in funzione di un qualsiasi AP wireless, anche se non esplicitamente connesso alla Rete dati, invii preventivamente all'Area ICT una richiesta sottoscritta dal responsabile, analogamente alla procedura seguita per le reti cablate.

Sono inoltre richieste le seguenti misure minime:

1. Devono essere operative tutte le misure necessarie per l'autenticazione dell'utente con credenziali personali e la memorizzazione degli accessi (log) secondo le modalità di legge.
2. Devono essere attribuiti indirizzi IP privati e deve essere consentita la navigazione solo attraverso proxy.
3. La navigazione su Internet deve essere consentita solo previa accettazione di liberatoria da parte dell'utente per il salvataggio dei log del proxy, sottoposti a trattamento dati in conformità con il GDPR.
4. Access Point e postazioni wireless devono costituire una rete separata (fisica o virtuale) del comprensorio/campus rispetto alle LAN di struttura.
5. Gli Access Point ad accesso libero che non richiedono alcuna forma di autenticazione da parte dell'utente devono essere adeguatamente riconfigurati a cura della struttura o rimossi.

6. Non è necessario che la comunicazione via etere venga criptata, purché l'utente venga messo a conoscenza dei rischi nel caso di utilizzo di protocolli insicuri attraverso un'informativa.

L'Area ICT effettua periodicamente il monitoraggio proattivo delle reti wireless. Gli AP che causano interferenze e gli AP non autorizzati potranno essere rimossi, previa comunicazione ai responsabili di Struttura.

Utilizzo infrastruttura wireless EDUROAM e GenuaWiFI

Eduroam (Education Roaming) è la rete wireless prioritaria dell'Ateneo che ha come scopo principale quello di fornire la connettività radio nei punti di aggregazione studentesca più significativi e in tutte le aule.

Gli utenti di un'istituzione aderente a EduRoam, come l'Università di Genova, che visitano un altro istituto aderente sono in grado di utilizzarne la rete locale wireless (WLAN) usando le stesse credenziali (nome utente e password) che userebbero nella propria istituzione d'appartenenza, senza la necessità di ulteriori formalità presso l'istituto ospitante.

Per accedere a Eduroam è preferibile seguire la procedura di configurazione guidata, disponibile alla pagina seguente:

http://ict.unige.it/wi-fi-istruzioniconfigurazione

La rete locale GenuaWifi è pensata per quegli utenti che utilizzano raramente la rete wireless di Ateneo e per gli ospiti che non dispongono di credenziali Eduroam.

Per la configurazione si può fare riferimento alla pagina seguente:

http://ict.unige.it/wifi-istruzioniconfigurazione#configurazione

Per richiesta assistenza, suggerimenti o chiarimenti, è possibile inviare una mail al seguente indirizzo:

helpwifi@unige.it

Sono presenti risposte alle domande più frequenti, al seguente URL:

https://ict.unige.it/wifi-faq

Regole Generali Telefonia di Ateneo

Il Sistema Telefonico di Ateneo è gestito internamente dall'Area ICT, che provvede ad assegnare, modificare e rimuovere utenze.

Allo stato attuale le utenze attive sono circa 6000, a cui vengono sommati i servizi IVR (acronimo di Risposte Vocali Interattive).

All'interno delle Strutture e dei Centri, sono presenti tecnologie miste, per il collegamento telefonico: possono essere di tipo VOIP (apparecchi connessi alla rete dati a cui è possibile collegare "in serie" una postazione PC), oppure di tipo analogico (apparecchi che sfruttano l'impianto tradizionale a doppino).

Una Struttura che ha intenzione di richiedere una nuova linea telefonica e/o un eventuale apparecchio, può inoltrare istanza scritta all'indirizzo retifonia@unige.it

Tale richiesta può essere effettuata dalle seguenti figure di riferimento:

- Dirigente dell'Area o Caposervizio in caso di richiesta proveniente da un'Area dell'Amministrazione Centrale.
- Direttore di Scuola/Dipartimento, Responsabile Amministrativo di Scuola/Dipartimento o Coordinatore Tecnico in caso di richiesta proveniente dalle Strutture Fondamentali;

Premesso che gli apparecchi telefonici VoIP non devono mai essere scollegati, **eventuali apparecchi non più utilizzati devono essere tempestivamente restituiti all'Area ICT,** che provvederà all'eventuale riassegnazione.
In caso di richiesta di assegnazione di una nuova linea collegata ad un nuovo telefono VoIP, da parte di una Struttura, l'Area ICT effettuerà un monitoraggio presso la stessa Struttura per rilevare eventuali apparecchi scollegati dalla rete. Ne verificherà l'eventuale inutilizzo presso la Struttura stessa, invitandola a rinnovarne l'impiego in caso di necessità.

La modalità d'uso delle linee è descritta al seguente URL:

https://ict.unige.it/telefonia#toc-modalit-du-lVQ6E4lz

Gli apparecchi telefonici VOIP sono, a tutti gli effetti, dispositivi di rete del costo commerciale superiore a 100 € e rientrano nella casistica evidenziata nel precedente paragrafo delle Disposizioni Generali; pertanto, l'utente che ne entra in possesso è tenuto a compilare il modulo presente alla pagina seguente:

https://ict.unige.it/telefonia

sotto la voce:

Modulo di assegnazione apparecchio telefonico VoIP (personale in possesso di credenziali Office 365 UNIGE attive).

L'utente diventa a tutti gli effetti responsabile dell'apparecchio affidato ed è tenuto a comunicare all'Area ICT, attraverso l'indirizzo e-mail retifonia@unige.it , eventuali necessità di spostamento dell'apparecchio, che potrà rimanere assegnato, anche in caso di trasferimento ad altro ufficio, anche di Strutture diverse.

In caso di smarrimento o furto, l'assegnatario provvederà ad effettuare regolare denuncia alle Forze dell'Ordine e a far pervenire a retifonia@unige.it copia della stessa.

Manutenzione delle postazioni telefoniche

In analogia con quanto definito per la rete dati, la manutenzione dell'infrastruttura telefonica è a carico dell'Area ICT nella distribuzione verticale ai piani degli edifici.

In caso di realizzazione nuove postazioni di lavoro e di ripristino guasti nell'infrastruttura "orizzontale", la Struttura ha piena autonomia di intervento.

Può rivolgersi ad imprese specializzate, che possano realizzare ed intervenire sul cablaggio, certificandone la qualità dell'impianto.

Procedura per la segnalazione guasti telefonici e richieste generiche sulla telefonia

La manutenzione degli apparecchi che presentano problemi, è affidata alla Società con cui l'Ateneo ha stipulato l'accordo quadro.

È possibile aprire una chiamata, utilizzando l'apposito numero verde dedicato; tutto il personale può chiamare il numero verde, in caso di necessità.

Tutte le indicazioni sono fornite alla seguente pagina:

https://ict.unige.it/segnalazioneguastitelefonici

Per tutte le altre richieste di ordine generico (attivazione nuova linea, richieste di attivazione deviazione, dismissione telefono, ecc....), è possibile rivolgersi all'indirizzo:

retifonia@unige.it

Tali richieste possono essere avanzate da Direttori di Struttura, Responsabili amministrativi, Referenti di Edificio.

E' possibile richiede deviazioni di chiamata da linea telefonica fissa, verso altra linea esterna, purché la richiesta rientri nelle casistiche riportate al seguente URL:

https://ict.unige.it/info-deviazioni

Nell'ottica di una razionalizzazione e valorizzazione delle risorse e delle attrezzature messe a disposizione dall'Ateneo nonché di una riduzione della spesa in materia di telefonia fissa e mobile, si richiamano di seguito alcune informazioni e alcune richieste.

- Le chiamate da interno fisso ad interno fisso (senza deviazione verso numeri esterni) non generano costi;
- Le chiamate da interno fisso a numero esterno generano un costo a consumo che varia se la destinazione è urbana, nazionale, cellulare, internazionale;
- Le chiamate da interno fisso ad interno fisso con deviazione su cellulare generano un costo a consumo come in 2);
- Le chiamate fra cellulari di servizio appartenenti allo stesso contratto sono comprese nel canone (Amministrazione centrale e Strutture fondamentali hanno contratti differenti); in ogni caso nel canone mensile sono compresi anche dei minuti di conversazione a pagamento;
- Le chiamate vocali attraverso Teams non generano costi.

Per quanto sopra siamo tutti invitati a chiamare le persone non presenti alla propria postazione di lavoro (cioè in prossimità dell'apparecchio telefonico fisso) attraverso Microsoft Teams che si raccomanda di attivare in orario di lavoro, oppure, se non è possibile usare Teams, usando il cellulare di servizio chiamando altro cellulare di servizio.

Regole per l'accesso alla Rete GenuaNET dall'esterno

L'Ateneo, tramite l'Area ICT, mette a disposizione del personale docente, tecnico-amministrativo nonché degli studenti strumenti e modalità per l'accesso ai servizi di Ateneo dall'esterno della Rete UNIGE.
Uno degli strumenti per realizzare una connessione sicura da qualsiasi punto della rete internet verso l'interno della rete universitaria è la VPN (Virtual Private Network) con fattori multipli di autenticazione: con questo strumento si ha la possibilità di accedere alle risorse informatiche

dell'Università da una sottorete classificata per tale scopo e appropriatamente monitorata e controllata mediante policy di sicurezza.

Qualora una Struttura intenda intraprendere soluzioni autonome di fornitura di accesso remoto, il responsabile della stessa deve darne preventiva comunicazione scritta all'Area ICT, garantendo l'adozione di tutte le misure atte a prevenire intrusioni e/o utilizzi illeciti e a conservare a norma di legge i dati relativi alle connessioni, sempre in conformità con le AUP di GARR e presentando un progetto che deve essere validato dall'Area ICT per i rischi e gli eventuali impatti sulla sicurezza della rete GenuaNET nel suo complesso.
L'utilizzo della VPN è la soluzione prioritaria anche per consentire le connessioni di entità terze (ditte ed Enti che collaborano a vario titolo con l'Ateneo), verso GenuaNet.
Non è consentito utilizzare i software per l'accesso e il controllo remoto delle postazioni (es. Anydesk, Teamviewer, Supremo, ecc...), che compromettono la sicurezza dell'infrastruttura, "bypassando" le difese perimetrali della rete Genuanet.
Eventualmente, le entità terze possono essere fornite di credenziali ad hoc per l'utilizzo della VPN UNIGE, previa comunicazione all'Area ICT attraverso i comuni canali.
Tali credenziali saranno nominative, per un utilizzo non continuativo e di scadenza concordata.

Le informazioni generali, relative all'utilizzo della VPN sono riportate al link:

https://ict.unige.it/accesso-vpn

Il software da utilizzare è FORTICLIENT VPN, che consente di instaurare una connessione diretta alla Rete possid'Ateneo, impiegando le proprie credenziali UNIGEPass.

Tutte le indicazioni per installare il software necessario, sono reperibili al seguente URL:

https://ict.unige.it/istruzioni-vpn

In caso di necessità, come per la parte wi-fi, viene di seguito riportato il link da cui consultare risposte alle domande più frequenti:

https://ict.unige.it/faq-vpn

Per ogni altro chiarimento, non rientrante nella casistica, è possibile scrivere una e-mail all'indirizzo:

assistenza@unige.it

Qualunque necessità non prevista dalle presenti linee guida, deve essere esposta e discussa preventivamente con l'Area ICT, attraverso i canali già definiti sopra.