Ministero dell'Istruzione dell'Università e della Ricerca
CONSERVATORIO DI MUSICA *"Stanislao Giacomantonio"*
Portapiana - Convento di S. Maria della Grazie – 87100 COSENZA
☎0984/709024 🖹0984/29224 - c.f. 80007270780
Sito Internet: portale.conservatoriodicosenza.it
Posta Ordinaria: cmcosenza@conservatoriodicosenza.it
Posta Certificata: conservatoriodicosenza@pec.it

prot. 8741 del 27/10/2020

Decreto Presidenziale

Il Presidente

Vista l'adesione alla proposta del Consortium Garr X con la conseguente implementazione della nuova rete in fibra ottica e l'attivazione del relativo contratto di abbonamento;

Visto il Regolamento Europeo per la Protezione dei Dati Personali 2016/679;

Visto il D.Lgs. 101/2018 per il recepimento delle norme di cui al RE 2016/679;

Vista la Legge 21.12.1999 n. 508 "Riforma delle Accademie di Belle Arti, dell'Accademia Nazionale di Danza, dell'Accademia Nazionale d'Arte Drammatica, degli Istituti per le Industrie Artistiche, dei Conservatori di Musica e degli Istituti Musicali Pareggiati";

Visto il D.P.R. n° 132 del 28/02/2003 concernente il Regolamento recante criteri per l'autonomia statutaria regolamentare ed organizzativa delle Istituzioni artistiche e musicali;

Visto lo Statuto del Conservatorio di Musica di Cosenza;

Visto il parere del Consiglio Accademico espresso nella seduta n.12 del 29 Settembre 2020 sul Regolamento in materia di configurazione del firewall, regole di accesso alla rete e suo utilizzo;

Visto il verbale del Consiglio di Amministrazione n.9 del 16/10/2020, con il quale è stato deliberato il Regolamento in materia di configurazione del firewall, regole di accesso alla rete e suo utilizzo

DECRETA

l’entrata in vigore del “Regolamento per la configurazione del firewall, regole di accesso alla rete e suo utilizzo”.

-Configurazione del firewall-

Art. 1
Il firewall è il componente di difesa e protezione necessario per garantire la sicurezza della nuova rete in fibra ottica e regolarne l’accesso. Vista la sua funzione, è opportuno fissarne le regole di configurazione.

Art. 2
L’elaborazione dei criteri di configurazione del firewall è approntata da un’apposita commissione formata dal Presidente, dal Direttore o da un suo delegato, dal Direttore amministrativo o da un suo delegato e dalla figura interna di riferimento per gli aspetti tecnici della rete del Conservatorio e di collegamento con il fornitore pro tempore del servizio di abbonamento alla connessione in fibra ottica così come definito dallo stesso fornitore nell’art.8.

Art. 3
La commissione, in merito ai suddetti criteri e in particolare alle categorie, ai siti e alle applicazioni a cui accedere o da escludere tramite firewall, acquisisce sia il parere del responsabile tecnico dell’azienda che ha in carico la manutenzione dello stesso firewall, sia, ove necessario, il parere del responsabile di settore del fornitore del servizio di abbonamento alla connessione in fibra ottica.

Art. 4
La commissione redige la lista di blocco e/o filtro delle categorie, dei siti e delle applicazioni anche consultando le procedure di sicurezza elaborate dal fornitore pro tempore del servizio di connessione e abbonamento, accogliendo totalmente o parzialmente, e se necessario modificandolo, l’elenco dettagliato fornito dal responsabile tecnico dell’azienda che ha in carico la configurazione e manutenzione dello specifico modello di firewall installato.

Art. 5
Unico caso di non utilizzo del firewall: nelle attività di concerti dal vivo a distanza e/o di attività didattiche in cui sia richiesta l’interazione strumentale in tempo reale e simultanea tra docente e studente, la relativa connessione momentanea di gestione dell’evento deve bypassare il firewall per evitare latenze eccessive nel flusso audio-video che comprometterebbero inevitabilmente l’efficacia della performance rendendone impossibile la realizzazione. La responsabilità dell’operazione è direttamente in carico alla figura tecnica di riferimento del Conservatorio.

Art. 6
La commissione, nel caso in cui dovesse cambiare il fornitore pro tempore del servizio di connessione e abbonamento alla rete in fibra ottica o l'azienda che gestisce la manutenzione del firewall, verifica se le regole di configurazione del firewall debbano essere sottoposte a revisione.

Art. 7
Nel caso in cui se ne ravvisasse la necessità, la commissione può proporre la modifica del presente regolamento.

Art. 8
L'allegato documento di gestione delle procedure di sicurezza elaborate dal fornitore pro tempore del servizio di connessione e abbonamento è parte integrante del presente regolamento.

-Regole di accesso alla rete e suo utilizzo-

Art. 1
La nuova rete in fibra ottica del Conservatorio riveste un ruolo fondamentale sia nell'implementazione e nel potenziamento dell'offerta formativa in presenza e on line, e sia nell'ampliamento ed efficientamento dei servizi amministrativi. Per garantirne il corretto uso a tutte le componenti istituzionali si rende necessaria l'adozione di un apposito regolamento.

Art. 2
Le regole di accesso e utilizzo della rete sono approntate da una specifica commissione formata dal Presidente, dal Direttore o da un suo delegato, dal Direttore amministrativo o da un suo delegato e dalla figura di riferimento tecnico del Conservatorio.

Art. 3
La commissione accoglie totalmente o parzialmente, e se necessario modificandola, la policy del fornitore pro tempore del servizio di connessione e abbonamento alla rete in fibra ottica acquisendo, ove necessario, sia il parere del responsabile tecnico dell'azienda che ha in carico la manutenzione della stessa rete, sia il parere del responsabile di settore del fornitore del servizio di abbonamento alla connessione in fibra ottica.

Art. 4
L'allegata policy di accesso alla rete e del suo utilizzo è parte integrante del presente regolamento.

Art. 5
L’accesso alla rete è consentito ai docenti, al personale amministrativo e agli studenti in possesso dell’account Eduroam.

Art. 6
Gli utilizzatori sono tenuti ad attenersi alla policy adottata.

Art. 7
Nel caso che ad utilizzare la rete siano enti esterni al Conservatorio, le regole di connessione saranno dettate da una apposita convenzione, sottoscritta tra le parti ed approvata dal Conservatorio.

Art. 8
La commissione, nel caso in cui dovessero cambiare:
-il fornitore pro tempore del servizio di abbonamento alla connessione in fibra ottica;
-il relativo protocollo di accesso alla rete;
-l’azienda che gestisce la manutenzione della stessa;
verifica se le regole di accesso e utilizzo debbano essere sottoposte a revisione.

Art. 9
Nel caso in cui se ne ravvisasse la necessità, la commissione può proporre la modifica del presente regolamento.

Art. 10
L’allegato documento di policy di accesso alla rete elaborato dal fornitore pro tempore del servizio di connessione e abbonamento è parte integrante del presente regolamento.

Prof. Luigino Filice

FILICE LUIGINO
27.10.2020
18:34:03 UTC

Testi dei due documenti allegati

-inizio testo allegato a “Configurazione del firewall” -

Gestione degli Incidenti di Sicurezza sulla rete GARR

Premesse

(versione rilasciata il 25 giugno 2020 contemporaneamente alla pubblicazione delle nuove AUP riportate di seguito)

Riferimenti per gli incidenti di sicurezza

Ogni entità collegata alla rete GARR deve nominare il proprio responsabile tecnico locale, l'APM (Access Port Manager). L'APM gestisce il collegamento con la rete GARR ed è la persona di riferimento tecnico presso il GARR per la sua istituzione anche per quanto riguarda la gestione degli incidenti di sicurezza. La definizione di APM è disponibile sul sito istituzionale GARR. [https://www.garr.it/it/comunita/la-comunita-garr/gli-apm].

Comunicazioni

Le comunicazioni emesse dal GARR-CERT verso i soggetti coinvolti si svolgono principalmente tramite posta elettronica, con firma PGP (cert.garr.it/it/pgp/garr-cert-pgp-keys).

Protezione da attacchi esterni distribuiti

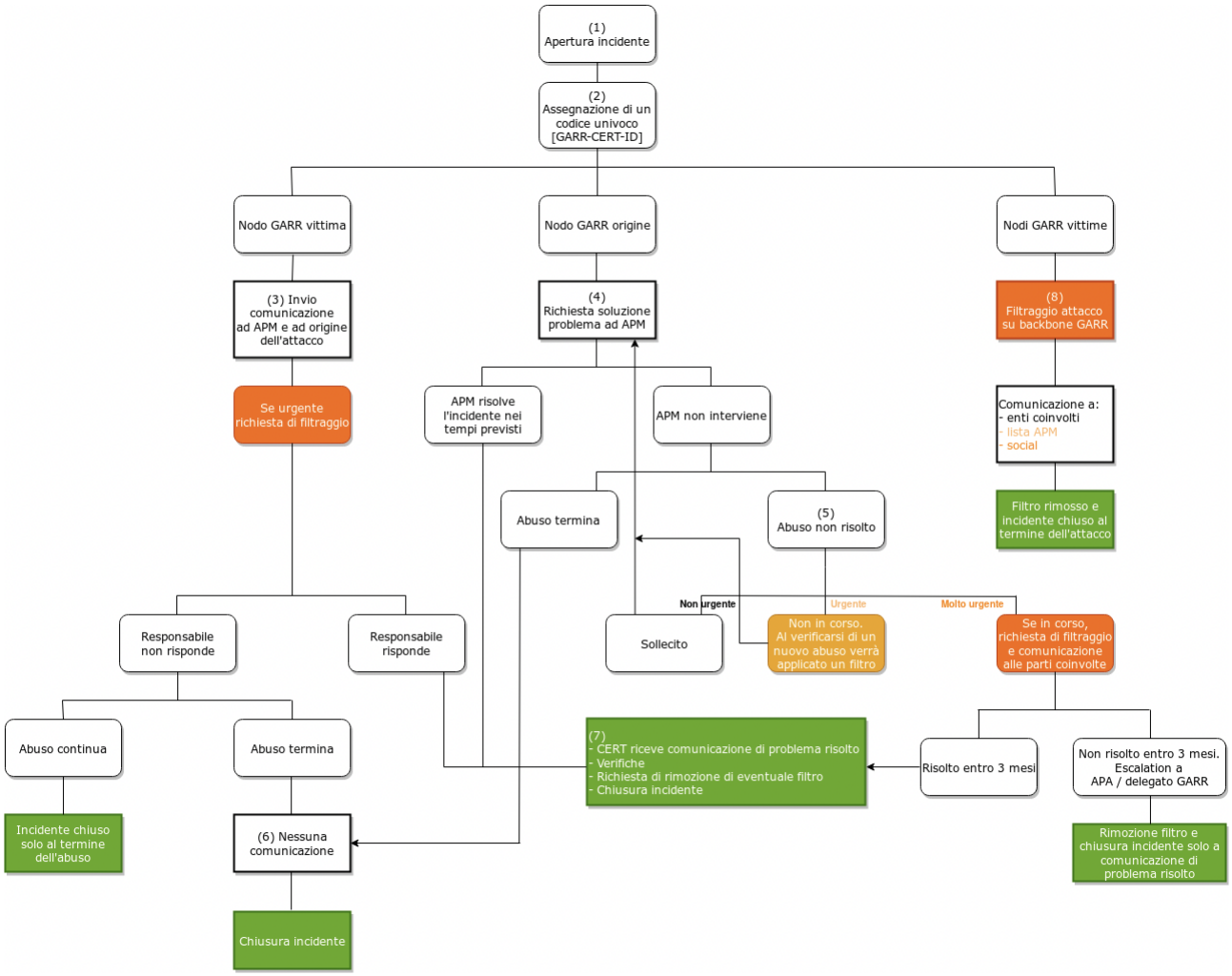
Da ottobre 2019, la rete GARR è dotata di un sistema automatico per la mitigazione di alcune tipologie di attacchi esterni, distribuiti e mirati a creare disservizi (DDoS - Distributed Denial of Service), basato su tecnologia Corero|Juniper (www.corero.com). Quando alcuni indicatori superano i valori di soglia, gli apparati di rete reagiscono ed eliminano selettivamente il traffico corrispondente a questo tipo di attacchi applicando dei filtri temporanei, permettendo così ai singoli nodi di mantenere normale funzionalità della rete. La procedura avviene in maniera automatica, senza nessun intervento da parte degli utenti. L'individuazione degli indicatori da utilizzare e i rispettivi valori di soglia sono configurati dal GARR-NOC.

Filtraggio

La gestione incidenti prevede, in alcuni casi particolari, il filtraggio di uno o più indirizzi di rete sulle interfacce dei router gestiti da GARR.
Ci preme sottolineare che l'applicazione di tali filtri è sempre da intendersi a protezione e salvaguardia della funzionalità della rete e dei servizi di connettività a disposizione degli utenti della rete GARR. Nel caso più evidente in cui gli IP GARR sono i bersagli diretti o indiretti di eventuali attacchi esterni, spesso sono gli stessi utenti (APM) a chiedere l'intervento del filtraggio al CERT/NOC per recuperare l'accesso ai loro dispositivi di frontiera e possibilmente intervenire sulle loro configurazioni per mitigare anche localmente il problema.

Nel caso in cui gli IP GARR siano sorgenti di traffico palesemente illecito e non vi sia alcuna risposta da parte dell'APM nei tempi previsti, gli IP coinvolti vengono filtrati da GARR (con i criteri descritti nella procedura di gestione degli incidenti di sicurezza), allo scopo di tutelare i propri utenti e prevenire da eventuali conseguenze legali. Dopo tre mesi dall'avvenuto filtraggio, in assenza di risposta da parte dell'APM, si procederà ad informare l'APA e il Delegato GARR dell'Ente di competenza (escalation).

Flusso della Procedura di Gestione Incidenti



Procedura di gestione incidenti adottata da GARR-CERT

1) Al verificarsi di un problema di sicurezza che veda coinvolto un soggetto appartenente alla rete GARR, GARR-CERT valuta l'apertura di un incidente di sicurezza e ne decide la priorità, le procedure di risoluzione e le modalità di comunicazione con i soggetti coinvolti.

2) GARR-CERT assegna all'incidente un codice univoco (Ticket ID).
• Nel caso in cui il soggetto GARR sia vittima dell'evento illecito, segue al punto 3. • Nel caso in cui il soggetto GARR sia origine dell'evento illecito, segue al punto 4. • Nel caso in cui l'evento illecito provenga da una o più sorgenti e sia destinato

contro più utenti GARR, segue al punto 8.

3) GARR-CERT invia all'APM una comunicazione informativa e ai contatti opportuni per il sistema origine dell'abuso.
In casi di particolare gravità ed urgenza, GARR-CERT valuta se richiedere un filtraggio temporaneo al GARR-NOC per mitigare l'attacco, quando non già applicato dal sistema di mitigazione automatica di DoS.

• Se l'abuso termina e il riferimento per il sistema che lo ha originato non risponde, segue al punto 6.

- Se il riferimento per il sistema che ha originato l'abuso risponde, segue al punto 7.
- L’incidente viene chiuso solo al termine dell’abuso.

4) GARR-CERT chiede all'APM di risolvere l'incidente entro un tempo commisurato alla gravità del caso (in calce alcuni esempi di tempistiche per tipologia di abuso). Quando possibile, fornisce anche indicazioni e suggerimenti utili. Se ritenuto opportuno, GARR-CERT risponde anche a coloro che hanno segnalato l'incidente.

  - Nel caso in cui l'APM intervenga entro i tempi richiesti, segue al punto 7.
  - Nel caso in cui l'APM non intervenga entro i tempi richiesti e l'abuso cessi, segue

    al punto 6.

  - Nel caso in cui l'APM non intervenga entro i tempi richiesti e l'abuso continui,

    segue al punto 5.

    5) GARR-CERT procede in uno dei seguenti modi, a seconda della gravità del caso:
    - Invia una mail di sollecito (2a comunicazione, ecc.) all'APM, invitandolo

      nuovamente ad intervenire. Tornare al punto 4.

- Invia un avviso di filtraggio all’APM (e in copia al GARR-NOC e alla direzione

GARR) nel quale è scritto che se l'evento illecito dovesse proseguire o ripresentarsi, il GARR-NOC provvederà ad applicare un filtraggio temporaneo opportuno, senza ulteriori preavvisi. Tornare al punto 4.

- Procede a richiedere l'applicazione di un filtro opportuno al GARR-NOC e, successivamente alla conferma di avvenuto filtraggio, avvisa l'APM e le altre parti coinvolte.

- Se entro tre mesi dall'applicazione del filtraggio l'APM interviene per risolvere il problema, segue al punto 7, altrimenti si procederà ad informare l'APA e il Delegato GARR dell'Ente di competenza; l’incidente quindi verrà chiuso e il relativo filtro rimosso solo in seguito alla comunicazione di avvenuta risoluzione.

6) GARR-CERT non riceve alcuna comunicazione: l’incidente viene chiuso d’ufficio.

7) GARR-CERT riceve la comunicazione di avvenuta risoluzione del problema e, quando tecnicamente possibile, procede alla verifica delle azioni intraprese prima di chiudere l’incidente ed avvisare tutte le parti coinvolte.
Nel caso in cui sia stato applicato un filtraggio da parte del NOC, il CERT ne richiede la rimozione e attende conferma prima di chiudere l’incidente.

8) Esaminato il tipo di attacco tramite gli strumenti di monitoraggio disponibili, CERT e NOC si coordinano per applicare un filtro sul backbone GARR. Viene inviata notifica ai contatti opportuni per la rete o le reti origine dell'abuso, agli utenti coinvolti, singolarmente o alla mailing list degli APM, ed eventualmente viene pubblicata la notizia seguendo i canali di comunicazione di GARR [web, social]. La chiusura dell'incidente e la rimozione dei filtri sul backbone sono subordinate alla verifica del termine dell'attacco.

Tipologia di incidenti trattati attualmente (con indicazione di tempistica d'intervento)

In funzione della tipologia, sono elencati i tempi richiesti per la risoluzione dell'incidente a partire dalla notifica. Nei casi in cui l'APM abbia bisogno di una dilazione dei tempi per risolvere l'incidente è necessario che ne faccia esplicita richiesta al GARR-CERT.

- Phishing (4 ore)
- DoS (5 ore)
- Connection Attempts (1 giorno)
- Compromised Node/Account (1 giorno) • Probe (1 giorno)
- Malware/Virus (1 giorno)
- Vulnerable Node/Account (3 giorni)
- Spam (3 giorni)
- Piracy (3 giorni)

In caso di emergenza

Nel caso si verifichi un incidente, anche fuori dall'orario di attività di NOC e CERT, che impatti significativamente sulla connettività degli utenti, come per esempio un SYNFlood distribuito, i responsabili di NOC e CERT decidono le modalità di:

a) applicazione di eventuali filtri a livello di router GARR anche entro tempi inferiori a quelli previsti nella Procedura di Gestione Incidenti,

b) comunicazione agli utenti coinvolti e, sentito il Direttore del Dipartimento Network [e/o il Direttore del GARR], se e come diffondere l'evento e i dettagli ad altri soggetti o pubblicamente.

Anche altri casi che espongano gli utenti a gravi problemi di sicurezza, ad esempio nel caso di data breach in corso che riguardano dati particolari, possono essere trattati a scopo cautelativo come al precedente punto (a).

Riferimenti normativi

L’aggiornamento della Procedura di Gestione Incidenti di Sicurezza del GARR e’ dovuta, oltre che all’evoluzione dei tipi di minacce sia esterne che interne alla rete e dei/ai sistemi degli utenti, anche all’evoluzione delle norme vigenti in Italia relative ai reati informatici.

Prima delle recenti direttive contenute nelle Misure Minime di Sicurezza per la Pubblica Amministrazione (AgID, 26/4/2016 - https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict) e del recepimento in Italia del Regolamento Europeo per la Protezione dei Dati Personali (D.lgs. 101/2018 - https://www.garanteprivacy.it/web/guest/provvedimenti/provvedimenti-a-carattere-generale), i reati informatici compaiono per la prima volta in Italia con la legge 547 del 1993, che introduce modificazioni e integrazioni del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica.

Questi sono, ad oggi, i reati informatici puniti dal Codice Penale:

- **Frode informatica** - Articolo 640 ter c.p. Consiste nell'alterare un sistema informatico

  per procurarsi un ingiusto profitto. Pena prevista: reclusione da sei mesi a tre anni e multa

  da 51 a 1.032 euro. Esempi: phishing.

- **Accesso abusivo ad un sistema informatico o telematico** - Articolo 615 ter c.p.

  Condotto da colui che si introduce in un sistema informatico o telematico protetto da misure di sicurezza, o vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Pena prevista: reclusione fino a tre anni. Secondo la giurisprudenza della Corte di Cassazione, commette il reato in esame colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto, violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso.

- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici** - Articolo 615 quater c.p. Punita con la reclusione fino a un anno e con la multa fino a 5.164 euro. Reato commesso da chi - al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno - abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico** - Articolo 615 quinquies c.p. Reclusione fino a due anni e multa sino a euro 10.329 per la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. Il reato è commesso da chi si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

- **Intercettazione, impedimento o interruzione illecita di comunicazioni** - Articoli 617 quater e 617 quinquies c.p. Viene sanzionato rispettivamente chi, senza essere autorizzato, intercetta, impedisce, interrompe o rivela comunicazioni informatiche e colui

che installa apparecchiature dirette ad intercettare, interrompere o impedire

comunicazioni informatiche.

- **Falsificazione, alterazione, soppressione di comunicazioni e danneggiamento di**

sistemi - Viene sanzionato dal codice penale anche chi falsifica, altera o sopprime la comunicazione informatica acquisita mediante l'intercettazione (articolo 617 sexies c.p.) e chi distrugge, deteriora, o cancella, dati, informazioni o programmi informatici (articolo 635 bis c.p.). E, con riguardo al reato di violazione e sottrazione di corrispondenza, la legge n. 547/1993, aggiornando l'articolo 616 c.p., precisa che per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza.

-fine testo allegato a “Configurazione del firewall”-

-inizio testo allegato a “Regole di accesso alla rete e suo utilizzo” -

Acceptable Use Policy – AUP

(Ultima versione approvata dal CdA del Garr il 25/06/2020)

1. La Rete Italiana dell’Università e della Ricerca, denominata comunemente "Rete GARR", si fonda su progetti di collaborazione di ricerca ed accademica tra le Università, le Scuole e gli Enti di Ricerca pubblici italiani. Di conseguenza il servizio di Rete GARR e gli altri servizi ad esso correlati, sono destinati principalmente alla comunità che afferisce al Ministero dell’Istruzione, dell'Università e della Ricerca. Esiste tuttavia la possibilità di estensione del servizio stesso anche ad altre realtà, quali quelle afferenti ad altri Ministeri che abbiano una Convenzione specifica con il Consortium GARR, oppure realtà che svolgono attività di ricerca in Italia, specialmente, ma non esclusivamente, in caso di organismi "no-profit" impegnati in collaborazioni con la comunità afferente al Ministero dell’Istruzione, dell’Università e Ricerca. L'utilizzo della Rete e dei suoi servizi è comunque soggetto al rispetto delle Acceptable Use Policy (AUP) da parte di tutti gli utenti GARR.
2. Il "Servizio di Rete GARR", definito brevemente in seguito come "Rete GARR", è costituito dall'insieme dei servizi di collegamento telematico, dei servizi di gestione della rete, dei servizi applicativi, di storage, di calcolo e di tutti quegli strumenti di interoperabilità (operati direttamente o per conto del Consortium GARR) che permettono ai soggetti autorizzati ad accedere alla Rete di comunicare tra di loro (Rete GARR nazionale). Costituiscono parte integrante della Rete GARR anche i collegamenti e servizi telematici che permettono la interconnessione tra la Rete GARR nazionale e le altre reti.
3. Sulla rete GARR non sono ammesse le seguenti attività:

- fornire a soggetti non autorizzati all'accesso alla Rete GARR il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing, di hosting e simili, nonché permettere il transito di dati e/o informazioni sulla Rete GARR tra due soggetti entrambi non autorizzati all'accesso sulla Rete GARR (third party routing);
- utilizzare servizi o risorse di Rete, storage o calcolo, collegare apparecchiature o servizi o software alla Rete, diffondere virus, hoaxes o altri programmi in un modo che danneggi, molesti o perturbi le attività di altre persone, utenti o i servizi disponibili sulla Rete GARR e su quelle ad essa collegate;

- creare o trasmettere o immagazzinare (se non per scopi di ricerca o comunque propriamente in modo controllato e legale) qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il genere, la razza o il credo;
- trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;
- danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password), chiavi crittografiche riservate e ogni altro “dato personale” come definito dalle leggi sulla protezione della privacy;
- usare le risorse e gli strumenti messi a disposizione dal GARR per fini principalmente commerciali quando non siano residuali rispetto alle attività istituzionali;
- svolgere sulla Rete GARR ogni altra attività vietata dalla Legge dello Stato, dalla normativa Internazionale, nonché dai regolamenti e dalle consuetudini ("Netiquette") di utilizzo delle reti e dei servizi di Rete cui si fa accesso.

4. La responsabilità del contenuto dei materiali prodotti e diffusi attraverso la Rete ed i suoi servizi è delle persone che li producono e diffondono. Nel caso di persone che non hanno raggiunto la maggiore età, la responsabilità può coinvolgere anche le persone che la legge indica come tutori dell’attività dei minori.
5. I soggetti autorizzati (S.A.) all’accesso alla Rete GARR, definiti nel documento "Regole di accesso alla Rete GARR", possono utilizzare la Rete ed i suoi servizi per tutte le proprie attività istituzionali. Si intendono come attività istituzionali tutte quelle inerenti allo svolgimento dei compiti previsti dallo statuto di un soggetto autorizzato, comprese le attività all'interno di convenzioni o accordi approvati dai rispettivi organi competenti, purché l'utilizzo sia a fini istituzionali. Rientrano in particolare nelle attività istituzionali, la attività di ricerca, la didattica, le funzioni amministrative dei soggetti e tra i soggetti autorizzati all'accesso e le attività di ricerca per conto terzi, con esclusione di tutti i casi esplicitamente non ammessi dal presente documento.
6. Tutti gli utenti a cui vengono forniti accessi alla Rete GARR ed ai suoi servizi devono essere riconosciuti ed identificabili. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati. Di norma gli utenti devono essere dipendenti del soggetto autorizzato, anche temporaneamente, all'accesso alla Rete GARR.
   Per quanto riguarda i soggetti autorizzati all'accesso alla Rete GARR (S.A.) gli utenti possono essere anche persone temporaneamente autorizzate da questi in virtù di un rapporto di lavoro a fini istituzionali. Sono utenti ammessi gli studenti regolarmente iscritti ad un corso presso un soggetto autorizzato con accesso alla Rete GARR.
7. È responsabilità dei soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR di adottare tutte le azioni ragionevoli per assicurare la conformità delle proprie norme con quelle qui esposte e per assicurare che non avvengano utilizzi non ammessi della Rete GARR. Ogni soggetto con accesso alla Rete GARR deve inoltre portare a conoscenza dei propri utenti (con i mezzi che riterrà opportuni) le norme contenute in questo documento.
8. I soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR ed ai suoi servizi accettano esplicitamente che i loro nominativi (nome dell'Ente, Ragione Sociale o equivalente) vengano inseriti in un annuario elettronico mantenuto a cura degli Organismi Direttivi del Consortium GARR.
9. In caso di accertata inosservanza di queste norme di utilizzo della Rete e dei suoi servizi, gli Organismi Direttivi del Consortium GARR prenderanno le opportune

misure, necessarie al ripristino del corretto funzionamento della Rete, compresa la sospensione temporanea o definitiva dell'accesso alla Rete GARR stessa.

10. I problemi di sicurezza che coinvolgono utenti e nodi della rete GARR sono gestiti con una Procedura di Gestione Incidenti, approvata dal Comitato Tecnico-Scientifico del Consortium GARR e consultabile all'indirizzo https://cert.garr.it/it/gestione-incidenti/procedura-di-gestione . La procedura potrà essere oggetto di aggiornamenti per garantire nel tempo la gestione ottimale degli incidenti di sicurezza.
11. L'accesso alla Rete GARR ed ai suoi servizi è condizionato all'accettazione integrale delle norme contenute in questo documento.

Altri soggetti, autorizzati ad un accesso temporaneo alla Rete (S.A.T.) potranno svolgere solo l'insieme delle attività indicate nell'autorizzazione.
Il giudizio finale sulla ammissibilità di una attività sulla Rete GARR resta prerogativa degli Organismi Direttivi del Consortium GARR.

-fine testo allegato a “Regole di accesso alla rete e suo utilizzo” -