Disciplinare
per l'uso delle risorse informatiche dell'INFN

Ottobre 2025

Rev. 26/10/2025

1. Principi generali

L'INFN considera le risorse di calcolo ed i servizi di rete, nonché i dati e le informazioni da questi trattati, parte integrante del proprio patrimonio e funzionali al raggiungimento delle proprie finalità istituzionali di ricerca scientifica e tecnologica.

Con il presente Disciplinare l'INFN intende salvaguardare la sicurezza del proprio sistema informatico e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati, anche personali, raccolti, prodotti o comunque trattati.

L'INFN, inoltre, aderendo all'associazione Consortium GARR - Rete italiana dell'Università e della Ricerca - e utilizzandone i relativi servizi e strumenti, intende assicurare, sempre tramite questo Disciplinare, la conformità delle proprie norme con quelle dettate dal Consortium GARR.

Nell'INFN il trattamento dei dati raccolti attraverso l'uso delle risorse di calcolo e dei servizi di rete avviene solo per finalità determinate, esplicite e legittime, nel rispetto dei principi di necessità, pertinenza, correttezza e non eccedenza, secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (**GDPR** nel seguito).

L'INFN, per il raggiungimento delle proprie finalità istituzionali, implementa, utilizza e gestisce sistemi di intelligenza artificiale nel rispetto di quanto previsto dalla normativa europea e nazionale tutelando i valori, le libertà, i diritti e l'autonomia dell'individuo che considera parte attiva e fondamentale del progresso umano e scientifico.

2. Ambito di applicazione

Il presente Disciplinare si applica a tutti coloro cui sia stato consentito l'accesso alle risorse informatiche dell'INFN.

Le norme di seguito esposte integrano i doveri minimi di condotta previsti nel Codice di Comportamento dell'INFN[1].

[1] https://l.infn.it/codicecomportamento

3. Definizioni

Per **risorse informatiche** si intendono:

- elaboratori e analoghi dispositivi elettronici, stampanti e altre periferiche di proprietà dell'Ente o comunque connesse alla rete dell'Ente;
- apparati e infrastrutture di rete di proprietà dell'Ente o comunque connessi alla rete dell'Ente;
- il servizio di connettività alle reti locali e geografiche con esclusione della mera connettività geografica garantita tramite accordi tra Istituzioni e Federazioni (ad es. eduroam);
- istanze virtuali di calcolatori o apparati di rete;
- basi di dati e sistemi per la loro gestione;
- infrastrutture e servizi erogati dalle Strutture dell'Ente e centralmente attraverso la Direzione Sistemi Informativi e i Servizi Nazionali della CCR;
- infrastrutture e servizi erogati o gestiti dall'Ente su cloud INFN (DataCloud) o su cloud esterne, anche commerciali;
- software e dati acquistati, prodotti o pubblicati dall'Ente;

I soggetti che operano con le risorse informatiche dell'Ente si distinguono in:

- **utente**: ogni soggetto che abbia accesso alle risorse informatiche dell'Ente, in relazione alle funzioni ed attività che svolge nell'ambito dell'Istituto;
- **utente privilegiato**: ogni soggetto che abbia credenziali di amministratore della risorsa individuale assegnata, senza essere nominato amministratore di sistema;
- **amministratore di sistema**: figura professionale, dotata di credenziali privilegiate, dedicata alla gestione e alla manutenzione degli impianti di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, i servizi web, le reti locali e gli apparati di sicurezza;
- **team responsabile delle risorse informatiche**: il gruppo cui compete la gestione e la sicurezza delle risorse informatiche, i collegamenti in rete all'interno ed all'esterno di ciascuna Struttura o diverso contesto, nonché la cura, l'installazione, lo sviluppo e l'assistenza; si intendono tali i Servizi di Calcolo presso le Strutture, la Direzione Sistemi Informativi (DSI), il gruppo di gestione di INFN DataCloud e ogni altro team che venga qualificato come tale da un organo dell'Istituto o dal Direttore di riferimento;
- **direttore di riferimento:** il direttore della Struttura cui afferiscono le risorse informatiche e il team responsabile delle stesse; nel caso di infrastrutture distribuite, la figura esplicitamente incaricata da un organo dell'Istituto.

4. Accesso alle risorse informatiche

L'accesso alle risorse informatiche dell'INFN è consentito, previa identificazione, ai dipendenti e agli associati, a collaboratori, ospiti, dottorandi, specializzandi, assegnisti, borsisti, laureandi, anche afferenti a enti, aziende o organizzazioni partner di INFN all'interno di progetti, collaborazioni, contratti, o altri autorizzati secondo le norme del presente Disciplinare.

L'identificazione deve avvenire tramite verifica di un documento di identità in corso di validità o tramite procedure o strumenti equivalenti.

L'accesso alle risorse è inoltre subordinato alla accettazione del presente disciplinare, delle regole

d'uso accessorie[2], eventuali ulteriori AUP e ToU specifici del servizio nonché al superamento di un corso di sicurezza informatica di livello adeguato alla criticità delle risorse[3].

L'accesso alle risorse è verificato tramite credenziali di autenticazione individuali.

Nel caso in cui l'accesso sia consentito a soggetti esterni all'INFN, l'identificazione, la verifica della competenza in sicurezza informatica e l'autenticazione possono essere demandati all'Organizzazione di afferenza, previo accordo inserito nel documento di collaborazione che garantisca il soddisfacimento dei requisiti sopra elencati.

L'autorizzazione all'accesso, per la durata del rapporto in base al quale è consentito l'utilizzo delle risorse informatiche dell'INFN, è rilasciata dal direttore di riferimento, o da un suo delegato.

L'accesso è personale e non può essere condiviso o ceduto.

5. Disposizioni generali

Le risorse informatiche sono asset essenziali per l'INFN, e sono rese disponibili per il conseguimento delle finalità istituzionali dell'Ente.

Gli utenti sono tenuti a servirsi delle risorse informatiche dell'Ente prestando il proprio contributo perché ne sia preservata l'integrità e garantito il buon funzionamento.

Sono pertanto vietate:

1. attività contrarie alla legge nazionale, comunitaria e internazionale;
2. attività proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti;
3. attività commerciali, o comunque lucrative, non autorizzate, nonché la trasmissione di materiale commerciale e/o pubblicitario non richiesto o l'uso delle proprie risorse da parte di terzi per tali attività;
4. attività idonee a danneggiare, distruggere o compromettere la sicurezza delle risorse informatiche dell'Ente o dirette a violare la riservatezza o cagionare danno a terzi, ivi inclusa la creazione, trasmissione e conservazione di immagini, dati o altro materiale offensivo, diffamatorio, osceno, indecente o che attenti alla dignità umana, specialmente se riguardante il sesso, l'etnia, la religione, le opinioni politiche, la condizione personale o sociale;
5. attività che possano nuocere alla reputazione dell'Ente;
6. attività comunque non conformi ai fini istituzionali dell'Ente.

L'utilizzo delle risorse informatiche per finalità personali è tollerato purché non violi le leggi applicabili, non interferisca con il corretto funzionamento delle infrastrutture, sia compatibile con le norme del presente Disciplinare e delle regole d'uso accessorie[2] e sia limitato in durata e frequenza.

6. Disposizioni specifiche per l'uso delle risorse informatiche

Per motivi di sicurezza informatica è vietato:

1. connettere risorse di calcolo alla rete locale o ad altri servizi che includono la connettività di rete senza l'autorizzazione del team responsabile delle risorse informatiche;
2. collegare apparati di rete o modificarne la configurazione senza l'autorizzazione del team responsabile delle risorse informatiche;
3. utilizzare indirizzi e nomi di rete senza l'autorizzazione del team responsabile delle risorse

[2] https://security.infn.it/computing-rules

[3] https://security.infn.it/computing-rules/formazione-sicurezza-informatica

informatiche;

4. installare sistemi, hardware o software, che consentano accesso alle risorse informatiche senza l'autorizzazione del team responsabile delle risorse informatiche;
5. fornire accesso alle risorse informatiche a soggetti non espressamente autorizzati;
6. divulgare informazioni classificate come riservate sulla struttura e configurazione delle risorse informatiche, in particolare quelle che consentono accesso da remoto;
7. accedere senza autorizzazione ai locali dedicati ad ospitare risorse di calcolo, nonché alle aree riservate alle apparecchiature di rete;
8. intraprendere qualsiasi azione diretta a degradare le risorse del sistema, impedirne l'accesso ai soggetti autorizzati, ottenere risorse superiori a quelle autorizzate o accedere alle risorse violandone le misure di sicurezza.

6.1 Utenti

Gli **utenti**, in aggiunta alle disposizioni già indicate:

1. sono tenuti ad agire nel rispetto delle indicazioni in materia di sicurezza informatica fornite dal Nucleo Cybersecurity dell'INFN (NUCS), dal team responsabile delle risorse informatiche nonché delle norme dettate dall'INFN per il trattamento dei dati personali reperibili nelle pagine web del DPO[4].
2. sono responsabili dei dati e del software che installano sulle risorse informatiche loro affidate, procedono a una loro attenta valutazione preliminare e non installano per nessuna ragione software privi delle regolari licenze;
3. sono tenuti a proteggere da accessi non autorizzati i dati utilizzati o memorizzati nei sistemi cui hanno accesso;
4. sono tenuti a proteggere il proprio account mediante password che rispettino le relative norme di sicurezza[5];
5. non devono diffondere né comunicare la propria password, ovvero concedere ad altri l'uso del proprio account;
6. sono tenuti a seguire le indicazioni del team responsabile delle risorse informatiche per il salvataggio periodico dei dati e programmi;
7. non devono aggirare le misure di isolamento e di sicurezza delle risorse assegnate;
8. sono tenuti a segnalare immediatamente al team responsabile delle risorse informatiche incidenti, sospetti abusi e violazioni della sicurezza;
9. devono utilizzare programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili prima del loro utilizzo;
10. non devono mantenere connessioni remote inutilizzate né abbandonare la postazione di lavoro con connessioni aperte non protette;
11. se utilizzano dispositivi mobili sono tenuti a rispettare le indicazioni del paragrafo **Dispositivi mobili**;
12. sono tenuti, al termine del rapporto con l'INFN a trasferire al proprio responsabile, o al direttore di riferimento o al soggetto da questo delegato, i dati relativi all'attività lavorativa e a cancellare gli altri;
13. devono rispettare ogni altra indicazione in materia che dovesse essere fornita dall'Ente.

[4] https://dpo.infn.it

[5] https://security.infn.it/computing-rules/password-policy

6.2 Utenti privilegiati

Gli **utenti privilegiati**, oltre a soddisfare le disposizioni precedenti**:**

1. devono prendere visione dei documenti con le norme tecniche d'uso per i dispositivi informatici individuali[6] e seguirne le indicazioni;
2. non possono dare accesso alle loro risorse ad altri utenti;
3. non devono interferire con il sistema di raccolta dei log;
4. devono utilizzare, sui sistemi che li supportano, programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili prima del loro utilizzo;
5. devono rispettare ogni altra indicazione che dovesse essere fornita dall'Istituto in materia.

6.3 Amministratori di sistema

Gli amministratori di sistema sono nominati individualmente dal direttore di riferimento o da figura da esso delegata. In caso di utenti esterni, la nomina può essere a cura dell'Organizzazione di afferenza, secondo le modalità indicate nell'accordo di collaborazione.

Gli **amministratori di sistema**, oltre a soddisfare le disposizioni precedenti, sono tenuti a:

1. mantenere i sistemi al livello di sicurezza appropriato al loro uso;
2. verificare con regolarità l'integrità dei sistemi;
3. controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;
4. dare accesso alle risorse assegnate solo dopo aver verificato che l'utente rispetti le condizioni indicate nel paragrafo **Accesso alle risorse informatiche**;
5. conservare l'associazione tra gli account e le identità degli utenti;
6. non condividere l'accesso privilegiato alle risorse assegnate;
7. segnalare immediatamente al team responsabile delle risorse informatiche incidenti, sospetti abusi e violazioni della sicurezza e partecipare alla loro gestione;
8. installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono;
9. non visionare dati personali o corrispondenza, salvo per necessità tecniche, e in generale considerare sempre tali informazioni strettamente riservate;
10. in caso di interventi di manutenzione da parte di supporto esterno, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;
11. seguire attività formative in materie tecnico-gestionali, di sicurezza delle reti, dei sistemi o dei servizi amministrati, e di protezione dei dati personali;
12. rispettare ogni altra indicazione in materia che dovesse essere fornita dall'Istituto.

6.4 Team responsabile delle risorse informatiche

Il **team responsabile delle risorse informatiche**:

1. ha in carico la gestione e la sicurezza delle risorse informatiche di propria competenza;
2. è tenuto a rispettare le indicazioni in materia di sicurezza informatica fornite dal Nucleo Cybersecurity dell'INFN (NUCS)

[6] https://security.infn.it/computing-rules

3. è tenuto a dare accesso alle risorse assegnate solo dopo aver verificato che l'utente rispetti le condizioni indicate nel paragrafo **Accesso alle risorse informatiche**;
4. controlla che gli accessi remoti alle risorse locali avvengano esclusivamente mediante l'uso di protocolli che prevedano l'autenticazione e la cifratura dei dati trasmessi;
5. disattiva i servizi non essenziali sulle macchine gestite e limita il numero degli utenti privilegiati a quello strettamente necessario per le attività di coordinamento, controllo e monitoraggio della rete e dei servizi ad essa afferenti;
6. effettua la revisione, almeno annuale, degli account;
7. effettua il monitoraggio della rete e dei sistemi gestiti, incluse le risorse utilizzate per l'erogazione di servizi di tipo cloud, per garantirne la funzionalità e la sicurezza;
8. realizza i sistemi di filtraggio e di log sugli apparati perimetrali della rete;
9. segnala immediatamente al NUCS gli incidenti di sicurezza;
10. fornisce supporto per conservare e incrementare la sicurezza delle risorse affidate agli utenti;
11. rispetta ogni altra indicazione in materia che dovesse essere fornita dall'Istituto.

7. Sistemi di intelligenza artificiale

L'impiego dei Sistemi di Intelligenza Artificiale deve assicurare il rispetto delle leggi vigenti e dei principi di economicità, efficacia, efficienza, imparzialità, pubblicità, trasparenza, correttezza, responsabilità, sicurezza, sostenibilità ambientale, non discriminazione, tutela della riservatezza dei dati personali e della proprietà intellettuale.

A tale scopo l'utilizzo della IA nell'INFN è consentito nel rispetto delle norme e di eventuali disciplinari o linee guida sviluppati appositamente.

Al fine di garantire il rispetto della riservatezza dei dati, anche in relazione al GDPR, l'utilizzo di strumenti di Intelligenza Artificiale esterni è equiparato all'utilizzo di servizi esterni in generale, e disciplinato nel paragrafo **Disposizioni per l'uso di servizi esterni.**

8. Disposizioni per l'uso dei servizi esterni

Il trattamento dei dati personali di qualunque tipo, o dati di particolare rilevanza per l'Ente, può essere effettuato mediante l'uso di servizi informatici forniti da soggetti esterni soltanto ove l'INFN, mediante il DPO, il team responsabile delle risorse informatiche o altre figure competenti in materia, abbia preventivamente verificato i rischi e i benefici connessi ai servizi offerti, i limiti nella circolazione e trasferimento dei dati, nonché l'affidabilità del fornitore, la sussistenza di garanzie e cautele per la conservazione, persistenza e confidenzialità dei dati nonché i profili di responsabilità nel trattamento e definito la qualificazione dei rapporti in relazione alla disciplina del GDPR.

Nel caso di servizi cloud destinati alle attività gestionali dell'Istituto, questi devono essere qualificati per l'uso da parte della Pubblica Amministrazione.

L'elenco dei servizi esterni approvati in funzione della tipologia di utilizzo[7] è mantenuto aggiornato dalla Commissione Calcolo e Reti.

[7] https://security.infn.it/computing-rules/servizi-esterni

9. Dati acquisiti in relazione all'uso delle risorse informatiche

L'INFN non consente l'installazione di strumentazioni hardware e software mirate al controllo degli utenti e vieta il trattamento effettuato mediante apparecchiature preordinate al controllo a distanza.

L'INFN vieta il trattamento dei dati personali acquisiti per qualsiasi motivo allo scopo di controllo e profilazione delle attività degli utenti, con le eccezioni e nei limiti di seguito indicati.

9.1 Dati utente

l'INFN mette a disposizione degli utenti sistemi per l'archiviazione dei propri dati che supportano strumenti per la protezione in lettura e scrittura. È responsabilità dell'utente adottare le necessarie configurazioni per proteggerli adeguatamente.

Il team responsabile delle risorse informatiche può accedere a tali dati in caso di malfunzionamenti, per salvare copie di sicurezza, o quando esplicitamente richiesto dall'utente stesso.

Tali informazioni possono contenere dati personali.

9.2 Backup e restore

Per garantire la resilienza dei dati di sistemi, servizi e utenti, il team responsabile delle risorse informatiche ne acquisisce e salva copia quotidiana e/o settimanale.

Questi dati possono contenere dati personali.

Questo trattamento viene effettuato unicamente allo scopo di ripristinare la disponibilità dei dati stessi in caso di necessità.

I backup vengono conservati per un periodo non superiore a 12 mesi, al termine del quale vengono cancellati definitivamente dai sistemi di storage.

9.3 Dati di log

Per garantire la funzionalità operativa dei sistemi e dei servizi informatici il team responsabile delle risorse informatiche acquisisce e salva dati di log delle applicazioni e delle connessioni di rete.

Tali dati possono contenere dati personali.

I log vengono salvati su sistemi accessibili al solo personale del team, e possono essere analizzati allo scopo di affrontare e risolvere eventuali malfunzionamenti o eventi di sicurezza informatica.

I log vengono conservati per un periodo di tempo non superiore a 6 mesi, al termine del quale vengono cancellati definitivamente.

9.4 Dati per la sicurezza informatica

Al fine di contrastare tentativi di accesso non autorizzato e supportare al meglio la protezione e la sicurezza di dati e servizi, il NUCS ed il team responsabile delle risorse informatiche possono acquisire in modo automatizzato informazioni relative alle configurazioni dei dispositivi connessi alle reti INFN, alle connessioni di rete ed alle attività degli utenti

Le informazioni raccolte, che possono contenere dati personali, vengono salvate su sistemi dedicati alla cybersicurezza, su risorse interne o su servizi cloud esterni. Se su cloud esterna, tali risorse ottemperano ai requisiti specificati nel paragrafo "**Disposizioni per l'uso dei servizi esterni**".

I dati relativi sono in esclusiva disponibilità del NUCS e del team responsabile delle risorse

informatiche e vengono trattati al solo scopo di individuare e gestire o prevenire incidenti di sicurezza informatica.

I dati vengono trattati da strumenti automatizzati. In caso di potenziale anomalia, i dati pertinenti vengono analizzati manualmente; in questo caso gli utenti coinvolti vengono informati su quanto di loro competenza ed eventualmente invitati a fornire ulteriori informazioni riguardo l'incidente.

Gli utenti devono collaborare con il personale del NUCS o del team e fornire tutti gli elementi a propria conoscenza.

I dati raccolti per le attività di sicurezza informatica vengono conservati per un periodo di tempo non superiore a 6 mesi, al termine del quale vengono cancellati definitivamente.

In caso di incidente di impatto rilevante i dati relativi possono venire conservati in modalità criptata per periodi più lunghi, per consentire l'adempimento degli obblighi conseguenti e favorire le verifiche e ispezioni da parte delle Autorità competenti

9.5 Posta elettronica

L'inoltro automatico dell'intera casella di posta elettronica INFN verso domini non INFN, in particolare verso domini commerciali non è consentito.

I metadati relativi alla posta elettronica (log) vengono trattati come descritto nel capitolo "**Dati di log**", ma per un periodo di tempo non superiore a 21 giorni.

La casella di posta elettronica è disattivata alla scadenza del termine di autorizzazione all'accesso alle risorse INFN, attivando se possibile un sistema che informi di indirizzi alternativi riferiti alla sua attività professionale.

Il contenuto della casella è cancellato entro 12 mesi dalla scadenza del termine di autorizzazione all'accesso. Questo periodo può essere prolungato dal Direttore di riferimento per motivate ragioni connesse alle esigenze di servizio.

9.6 Dati particolari

Ai sensi del GDPR, i dati personali che rivelino l'origine etnica, le opinioni politiche, le convinzioni religiose, filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute, alla vita o all'orientamento sessuale, a condanne penali e reati richiedono un livello più elevato di sicurezza e di tutela.

Il trattamento di dati personali e di dati particolari viene effettuato solo da personale esplicitamente incaricato e adeguatamente formato.

La trasmissione di dati particolari deve comunque essere sempre effettuata utilizzando protocolli di cifratura allo stato dell'arte, secondo le policy definite nei documenti accessori[8].

Nel caso di trattamento di dati genetici, deve essere garantita, oltre alle disposizioni previste dal GDPR, la normativa nazionale di attuazione. A tale scopo, il trattamento di dati genetici, anche a fini di ricerca, viene autorizzato solo su infrastrutture ed a personale esplicitamente qualificati. Le infrastrutture INFN a questo dedicate devono essere qualificate tramite certificazioni standard ISO.

[8] https://security.infn.it/computing-rules/policy-crittografia

9.7 Accesso urgente ed improrogabile ad informazioni di servizio

Qualora fosse necessario ed improrogabile accedere a dati o messaggi inerenti l'attività lavorativa in possesso esclusivo dell'utente, e solo in caso di prolungata irreperibilità o grave impedimento, il direttore di riferimento o un suo delegato può accedere ai dati e messaggi dell'utente per individuare ed estrarre le informazioni rilevanti per lo svolgimento dell'attività lavorativa.

Di questa attività verrà redatto un verbale e l'utente verrà informato se e appena possibile.

9.8 Scadenza del rapporto di lavoro o collaborazione

Alla cessazione del rapporto di lavoro o di collaborazione l'accesso alle risorse informatiche viene revocato. Entro tale termine l'utente ha il dovere di rendere disponibili i dati di collaborazione ai colleghi e di trasferire altrove i dati personali.

Su richiesta dell'utente il direttore di riferimento può autorizzare una estensione dell'accesso per un periodo massimo di due mesi al solo scopo di completare questi trasferimenti.

Entro il termine di 12 mesi dalla cessazione del rapporto di lavoro o collaborazione, l'INFN provvede alla cancellazione dei dati presenti sulle risorse informatiche riferibili all'utente.

In caso di grave indisponibilità o decesso dell'utente, il Direttore di riferimento, su richiesta, potrà rendere disponibile agli aventi diritto i dati con contenuti personali nelle ipotesi e secondo le modalità previste dalla normativa vigente.

10. Dispositivi mobili

L'uso di dispositivi mobili comporta specifici rischi legati alla loro portabilità e al loro utilizzo anche per uso privato.

L'INFN adotta le misure necessarie ad ottemperare agli obblighi del presente Disciplinare sui dispositivi mobili di proprietà dell'Ente (COPE). L'utente assegnatario del dispositivo COPE è ritenuto responsabile di eventuali danni cagionati per un uso negligente o nel caso abbia ridotto o eliminato le misure di sicurezza adottate dall'Ente.

Al fine di tutelare la privacy dei dipendenti, la sicurezza delle infrastrutture dell'Ente e dei dati trattati in relazione all'attività lavorativa, l'uso di dispositivi mobili personali (BYOD) per finalità connesse all'attività lavorativa è consentito esclusivamente previa accettazione e osservanza delle politiche specifiche in materia di gestione dei dispositivi, di sicurezza dei dati e delle reti, delle modalità accettabili di utilizzo, del backup e del ripristino dei dati[9].

11. Ulteriori misure per la tutela dei sistemi informativi

Al fine di assicurare la funzionalità, disponibilità, ottimizzazione, sicurezza ed integrità dei sistemi informativi e prevenire utilizzazioni indebite l'INFN, previa apposita informativa da rendere ai sensi del GDPR, adotta misure che consentono la verifica di comportamenti anomali o delle condotte non consentite dal presente Disciplinare, nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati. A tal fine, il team responsabile delle risorse informatiche o il NUCS possono eseguire elaborazioni sui dati registrati per rilevare anomalie nel traffico di rete o condotte non consentite.

Nel caso in cui si verifichino eventi dannosi o si rilevino comportamenti non consentiti, il team

[9] https://security.infn.it/computing-rules/dispositivi-mobili

responsabile delle risorse informatiche o il NUCS eseguono, previa informazione agli interessati e salvo i casi di necessità e urgenza, ulteriori accertamenti e adottano le misure necessarie ad interrompere le condotte dannose o non consentite.

Nei casi di reiterazione di comportamenti vietati o di particolare gravità, il team responsabile delle risorse informatiche adotta tutte le misure tecniche necessarie, dandone immediata comunicazione al direttore di riferimento, che dispone gli ulteriori provvedimenti ai sensi del paragrafo "**Violazione delle norme**".

12. Violazione delle norme

Ogni condotta attuata in violazione del presente Disciplinare potrà determinare la sospensione dell'accesso alle risorse informatiche, salvo eventuali azioni disciplinari, civili o penali.

La violazione delle disposizioni del presente Disciplinare che cagioni a terzi un danno risarcito dall'INFN potrà determinare l'esercizio del diritto di rivalsa nei confronti del responsabile, nelle forme e limiti stabiliti dalla legge.

13. Disposizioni finali

Il presente Disciplinare abroga e sostituisce integralmente tutti i precedenti regolamenti adottati in materia.

L'INFN assicura al presente Disciplinare e ai suoi successivi aggiornamenti la più ampia diffusione presso gli utenti mediante pubblicazione nella pagina web di ciascuna Struttura, nonché consegnandolo a ciascuno in modalità elettronica o cartacea, idonee comunque a dimostrarne l'avvenuta consegna.

I documenti accessori citati nei paragrafi precedenti, oltre ad altri che si possano rendere necessari a seguito delle evoluzioni tecnologiche, costituiscono parte integrante del presente Disciplinare.

Tali documenti sono aggiornati dalla Commissione Calcolo e Reti di concerto con il Responsabile della Transizione Digitale e sono disponibili all'indirizzo: https://security.infn.it/computing-rules.

14. Clausola di revisione

Il presente Disciplinare è aggiornato periodicamente in relazione all'evoluzione della tecnologia e della normativa di settore.