ISTITUTO NAZIONALE DI FISICA NUCLEARE

CONSIGLIO DIRETTIVO

DELIBERAZIONE N. 15442

Il Consiglio Direttivo dell'Istituto Nazionale di Fisica Nucleare, riunitosi a Roma in data 28 febbraio 2020, alla presenza di n. 31 dei propri componenti su un totale di 34,

- vista la propria deliberazione n. 14026 del 31 marzo 2016 con la quale è stato approvato il Disciplinare per l'uso delle risorse informatiche dell'INFN;
- visto il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27.4.2016 (di seguito anche Regolamento) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- visto il Decreto Legislativo 30.6.2003, n. 196 e s.m.i. recante il *"Codice in materia di protezione dei dati personali"*;
- vista la deliberazione di questo Consiglio n. 14844 del 27 luglio 2018 che ha definito l'organizzazione del trattamento dei dati personali all'interno dell'INFN;
- visto il Decreto Legislativo 7.3.2005, n. 82 e s.m.i. recante il *"Codice dell'amministrazione digitale"*;
- visto il Codice di Comportamento dell'INFN, approvato con Deliberazione di questo Consiglio n. 13352 del 26.9.2014;
- visto il Decreto Legislativo 14.9.2015, n. 151 che ha modificato l'art. 4 della Legge 20.5.1970, n. 300, in tema di tutela della libertà e dignità dei lavoratori nei luoghi di lavoro;
- viste le circolari n. 1/2017 e n. 2/2017 con le quali l'Agenzia per l'Italia Digitale ha individuato le *"Misure minime di sicurezza ICT per le pubbliche amministrazioni"* sulla base della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015;
- viste le circolari n. 2/2018 e n. 3/2018 con le quali l'Agenzia per l'Italia Digitale ha individuato, rispettivamente, *"Criteri per la qualificazione dei Cloud Service Provider per la PA"* e *"Criteri per la qualificazione di servizi SaaS per il Cloud della PA"*;
- ritenuto opportuno procedere ad un aggiornamento del Disciplinare in relazione all'evoluzione della tecnologia e della normativa di settore e tenuto conto delle esperienze applicative maturate dalla sua entrata in vigore;
- considerato prioritario incrementare l'efficienza e la sicurezza delle risorse di calcolo e servizi di rete, nonché la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati prodotti, raccolti o comunque trattati nell'INFN;

- viste le proposte di modifica al Disciplinare per l'uso delle risorse informatiche elaborate dal Gruppo di lavoro *Harmony*;
- preso atto del parere favorevole alle modifiche proposte espresso dalla Commissione Nazionale Calcolo e Reti il 28 gennaio 2020;
- sentito il DPO dell'INFN;
- ritenuto opportuno individuare un congruo termine per l'entrata in vigore delle modifiche;
- ritenuto che la formazione di tutti gli utenti e di quanti - anche con ruoli specifici - hanno accesso alle risorse informatiche e ai servizi di rete dell'INFN concorra al raggiungimento dei riferiti obiettivi di tutela, efficienza e sicurezza;
- visto il programma del corso e-learning base (di seguito corso) per la sicurezza informatica, elaborato nell'ambito della Commissione Nazionale Calcolo e Reti;
- ritenuto opportuno stabilire l'obbligatorietà del corso di cui al precedente capoverso per tutti gli utenti delle risorse informatiche e ai servizi di rete dell'INFN;
- ritenuto opportuno affidare nella Commissione Nazionale Calcolo e Reti, d'intesa con la Divisione Sistema Informativo dell'Amministrazione Centrale, la definizione delle misure organizzative necessarie all'erogazione del corso;
- tenuto conto che l'esecuzione della presente deliberazione non comporta oneri aggiuntivi di bilancio;
- visto l'articolo 12, comma 4, lettera i) dello Statuto dell'Istituto Nazionale di Fisica Nucleare in materia di attribuzioni del Consiglio Direttivo;
- acquisito il parere della Giunta Esecutiva;
- con voti favorevoli n. 31 componenti

DELIBERA

1. di approvare le modifiche al Disciplinare per l'uso delle risorse informatiche dell'INFN, come indicate nella tabella allegata, parte integrante alla presente deliberazione;

2. di individuare nel 16 marzo 2020 la data di entrata in vigore delle modifiche di cui al precedente capoverso;

3. di approvare il corso e-learning base per la sicurezza informatica, secondo il programma allegato, disponendo che lo stesso sia seguito sulla piattaforma a tal fine predisposta da tutti gli utenti delle risorse informatiche e ai servizi di rete dell'INFN;

4. di affidare alla Commissione Nazionale Calcolo e Reti, d'intesa con la Divisione Sistema Informativo dell'Amministrazione Centrale, la definizione delle misure organizzative necessarie per la partecipazione al corso.

Disciplinare per l'uso delle risorse informatiche nell'INFN

10 MARZO 2016	24 Gennaio 2020
1. Principi generali	**1. PRINCIPI GENERALI**
idem	*idem*
5. Nell'INFN il trattamento dei dati raccolti in relazione all'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. I sistemi informativi e i programmi informatici sono pertanto configurati in modo da ridurre al minimo l'utilizzo dei dati personali e identificativi.	5. Nell'INFN il trattamento dei dati raccolti in relazione all'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**. I sistemi informativi e i programmi informatici sono pertanto configurati in modo da ridurre al minimo l'utilizzo dei dati personali e identificativi.
idem	*idem*

6. Disposizioni specifiche per l'uso delle risorse informatiche	**6. DISPOSIZIONI SPECIFICHE PER L'USO DELLE RISORSE INFORMATICHE**
Gli Utenti inoltre:	2. Gli Utenti inoltre:
1. sono tenuti ad agire in conformità alla legge e nel rispetto delle indicazioni del Servizio di Calcolo e Reti in materia di sicurezza, garantendo la riservatezza nel trattamento dei dati personali, anche mediante la puntuale osservanza delle norme dettate dall'INFN in materia e accessibili presso la seguente pagina web: www.infn.it/privacy/;	1. sono tenuti ad agire in conformità alla legge e nel rispetto delle indicazioni del Servizio di Calcolo e Reti in materia di sicurezza, garantendo la riservatezza nel trattamento dei dati personali, anche mediante la puntuale osservanza delle norme dettate dall'INFN in materia e **pubblicate nelle pagine web del DPO INFN e dei Servizi Calcolo e Reti delle Strutture**;
idem	*idem*
7. sono tenuti a proteggere il proprio account mediante password non banali e, qualora siano presenti più sistemi di autenticazione, differenti per ogni sistema;	7. sono tenuti a proteggere il proprio account mediante password **che rispettino le norme di sicurezza indicate dall'Ente e dal Servizio Calcolo** e, qualora siano presenti più sistemi di autenticazione, differenti per ogni sistema; *idem*. **12. sono tenuti, al termine del rapporto di lavoro/collaborazione con l'INFN a trasferire al proprio responsabile, o al Direttore di Struttura o al soggetto da questo delegato, i file di contenuto inerente l'attività di servizio/collaborazione e a cancellare in via definitiva eventuali altri file. Entro il termine di due mesi dalla cessazione del rapporto, l'INFN provvede alla cancellazione dei dati presenti sulle risorse informatiche riferibili all'utente secondo le modalità indicate nel provvedimento del Garante per la tutela dei dati personali del 13 ottobre 2008. In caso di impossibilità o impedimento dell'Utente, ovvero laddove lo stesso, prima della cessazione del rapporto, non abbia reso disponibili i file attinenti**

	l'attività di servizio/collaborazione e non abbia delegato un collega a inoltrarli, il Direttore, o un suo delegato, può accedere alle risorse assegnategli per il periodo necessario a recuperare i dati di interesse. In caso di grave improvvisa indisponibilità o decesso dell'Utente, il Direttore, su richiesta, potrà rendere disponibile agli aventi diritto i file con contenuti personali. **Gli Utenti che hanno privilegi di amministratore sui loro sistemi (p.e. laptop) sono tenuti a prendere visione dei relativi documenti con le Norme d'uso, in attuazione della Circolare AgID 18/04/2017 n. 2/2017, e a seguirne scrupolosamente le indicazioni**.
7. Compiti del Referente di gruppo di utenti	**7. INDIVIDUAZIONE E COMPITI DEL REFERENTE DI GRUPPO DI UTENTI** **Il Referente del gruppo di utenti è individuato dal Direttore della Struttura cui afferisce in ragione delle funzioni assegnate. Il Referente può essere altresì individuato dalla collaborazione scientifica cui appartiene. La designazione è comunicata al Servizio di Calcolo e Reti competente.**
8. Compiti degli Amministratori di sistema	**8. INDIVIDUAZIONE E COMPITI DEGLI AMMINISTRATORI DI SISTEMA** **Gli Amministratori di Sistema sono designati dal Direttore della Struttura di afferenza con apposito atto.** **Nel caso in cui l'attività dell'Amministratore di Sistema riguardi risorse informatiche collocate presso più Strutture, l'atto di designazione è comunicato al Direttore e al Servizio di Calcolo e Reti di ciascuna Struttura.**

14. Violazione delle norme	**14. VIOLAZIONE DELLE NORME**
Ogni condotta posta in essere in violazione del presente Disciplinare determinerà la sospensione dell'accesso alle risorse di rete, salvo eventuali azioni disciplinari, civili o penali.	Ogni condotta posta in essere in violazione del presente Disciplinare **potrà determinare** la sospensione dell'accesso alle risorse di rete, 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, nei confronti del responsabile, l'esercizio del diritto di rivalsa nelle forme e nei limiti stabiliti dalla legge**.

Disciplinare per l'uso delle risorse informatiche nell'INFN

24 Gennaio 2020

1. PRINCIPI GENERALI

L'Istituto Nazionale di Fisica Nucleare (INFN) è un ente pubblico nazionale di ricerca disciplinato dalle norme contenute nel proprio Statuto.

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, da questo prodotti, raccolti o comunque trattati.

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

Nell'INFN il trattamento dei dati raccolti in relazione all'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. I sistemi informativi e i programmi informatici sono pertanto configurati in modo da ridurre al minimo l'utilizzo dei dati personali e identificativi.

Tutti coloro ai quali è consentito l'accesso alle risorse di calcolo e ai servizi di rete sono tenuti al rispetto delle norme di seguito esposte, che definiscono ed integrano i doveri minimi di condotta previsti nel Codice di Comportamento dell'INFN, oltre comunque a un comportamento ispirato ai principi di correttezza e diligenza.

2. AMBITO DI APPLICAZIONE

Il presente Disciplinare si applica a tutti coloro cui sia stato consentito l'accesso alle risorse di calcolo ed ai servizi di rete dell'INFN.

3. DEFINIZIONI

Per **risorse di calcolo** e **servizi di rete** si intendono:

- elaboratori e analoghi dispositivi elettronici, stampanti e altre periferiche (ad es. *scanner* e sistemi di storage) 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;
- software e dati acquistati, prodotti o pubblicati dall'Ente.

Nell'ambito del presente Disciplinare le risorse di calcolo ed i servizi di rete possono essere collettivamente definite **risorse informatiche**.

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

- **Utente**: ogni soggetto che abbia accesso alle risorse di calcolo e ai servizi di rete dell'INFN, in relazione alle funzioni ed attività che svolge nell'ambito dell'Istituto;
- **Referente di gruppo di utenti**: un soggetto che coordina gli utenti e l'uso delle risorse locali di uno o più gruppi, esperimenti o servizi, in conformità alle indicazioni del Servizio di Calcolo e Reti;
- **Amministratore di sistema**: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza;
- **Servizio di Calcolo e Reti**: il servizio cui compete la gestione delle risorse di calcolo centrali, i collegamenti in rete all'interno ed all'esterno di ciascuna Struttura, nonché la cura, installazione e sviluppo delle stesse e l'assistenza agli utenti per l'accesso alle risorse ed alla rete; ha inoltre competenza in materia di sicurezza su ogni risorsa di calcolo comunque afferente alla propria Struttura;
- **Direttore di Struttura**: il soggetto al quale, nel rispetto degli indirizzi approvati dal Consiglio Direttivo, compete la responsabilità di assicurare il funzionamento scientifico, organizzativo ed amministrativo di ciascuna Struttura come individuata nelle norme dello Statuto INFN.

4. ACCESSO ALLE RISORSE INFORMATICHE

L'accesso alle risorse di calcolo e ai servizi di rete dell'INFN è consentito, previa identificazione, ai dipendenti e agli associati, nonché a collaboratori, ospiti, dottorandi, specializzandi, assegnisti, borsisti, laureandi o altri autorizzati secondo le norme del presente Disciplinare.

L'autorizzazione all'accesso è rilasciata dal Direttore di Struttura o da un suo delegato per un periodo temporale limitato alla durata del rapporto sulla base del quale è consentita l'attività all'interno dell'INFN.

L'accesso è personale, non può essere condiviso o ceduto e il relativo utilizzo è consentito a ciascun utente soltanto in conformità alle norme del presente Disciplinare.

5. DISPOSIZIONI GENERALI PER L'USO DELLE RISORSE INFORMATICHE

Le risorse informatiche, in quanto essenziali per l'INFN, 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 affinché ne sia preservata l'integrità e garantito il buon funzionamento.

Sono pertanto vietate:

1. attività contrarie alla legge nazionale, comunitaria e internazionale o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti;
2. attività commerciali, o comunque lucrative, non autorizzate, nonché la trasmissione di materiale commerciale e/o pubblicitario non richiesto (spamming) o l'uso delle proprie risorse da parte di terzi per tali attività;
3. attività comunque idonee a danneggiare, distruggere, compromettere la sicurezza delle risorse informatiche dell'Ente o dirette a violare la riservatezza e/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, la razza, la religione, le opinioni politiche o la condizione personale o sociale;
4. 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 e sia compatibile con le norme del presente Disciplinare e di tutte le indicazioni stabilite dall'INFN.

6. DISPOSIZIONI SPECIFICHE PER L'USO DELLE RISORSE INFORMATICHE

Al fine di garantire la sicurezza delle risorse di calcolo e dei servizi di rete è vietato:

1. connettere risorse di calcolo alla rete locale o ad altri servizi che includono la connettività di rete senza l'autorizzazione del Servizio di Calcolo e Reti;
2. cablare, collegare o modificare apparati di rete senza l'autorizzazione del Servizio di Calcolo e Reti;
3. utilizzare indirizzi di rete e nomi non espressamente assegnati;
4. installare sistemi, hardware o software, che consentano accesso alle risorse informatiche senza l'autorizzazione del Servizio di Calcolo e Reti;

5. fornire accesso alle risorse informatiche a soggetti non espressamente autorizzati;
6. divulgare informazioni sulla struttura e configurazione delle risorse informatiche, con particolare riferimento a quelle che consentono accesso da remoto;
7. accedere senza autorizzazione ai locali del Servizio di Calcolo e Reti, nonché ai locali ed alle aree riservate alle apparecchiature di rete;
8. intraprendere ogni altra azione diretta a degradare le risorse del sistema, impedire ai soggetti autorizzati l'accesso alle risorse, ottenere risorse superiori a quelle autorizzate o accedere alle risorse di calcolo violandone le misure di sicurezza.

Gli **Utenti** inoltre:

1. sono tenuti ad agire in conformità alla legge e nel rispetto delle indicazioni del Servizio di Calcolo e Reti in materia di sicurezza, garantendo la riservatezza nel trattamento dei dati personali, anche mediante la puntuale osservanza delle norme dettate dall'INFN in materia e pubblicate nelle pagine web del DPO INFN e dei Servizi Calcolo e Reti delle Strutture.
2. nella scelta degli strumenti informatici di cui si servono, devono tenere in opportuna considerazione le indicazioni del Servizio di Calcolo e Reti, in particolare per quanto riguarda le caratteristiche relative alla sicurezza, privilegiando i sistemi e le procedure che offrono i livelli più elevati di protezione;
3. sono responsabili dei dati e del software che installano sui computer loro affidati: procedono ad una loro attenta valutazione preliminare e non installano software privi delle regolari licenze;
4. sono tenuti a proteggere da accessi non autorizzati i dati utilizzati e/o memorizzati nei propri computer e nei sistemi cui hanno accesso;
5. valutano attentamente l'affidabilità dei servizi esterni eventualmente utilizzati, ivi inclusi quelli di tipo *cloud*, in termini di sicurezza, conservazione e confidenzialità dei dati;
6. sono tenuti a seguire le indicazioni del Servizio di Calcolo e Reti per il salvataggio periodico dei dati e programmi utilizzati;
7. sono tenuti a proteggere il proprio account mediante password che rispettino le norme di sicurezza indicate dall'Ente e dal Servizio Calcolo e, qualora siano presenti più sistemi di autenticazione, differenti per ogni sistema;
8. non devono diffondere né comunicare la propria password, ovvero concedere ad altri l'uso del proprio account;
9. sono tenuti a segnalare immediatamente al proprio Referente e al Servizio di Calcolo e Reti incidenti, sospetti abusi e violazioni della sicurezza;
10. per i sistemi operativi che lo prevedono, devono utilizzare programmi antivirus aggiornati, avendo cura di sottoporre a scansione antivirus file e programmi scambiati via rete e i supporti rimovibili utilizzati;
11. non devono mantenere connessioni remote inutilizzate né abbandonare la postazione di lavoro con connessioni aperte non protette.
12. sono tenuti, al termine del rapporto di lavoro/collaborazione con l'INFN a trasferire al proprio responsabile, o al Direttore di Struttura o al soggetto da questo delegato, i file di contenuto inerente l'attività di servizio/collaborazione e a cancellare in via definitiva eventuali altri file. Entro il termine di due mesi dalla cessazione del

rapporto, l'INFN provvede alla cancellazione dei dati presenti sulle risorse informatiche riferibili all'utente secondo le modalità indicate nel provvedimento del Garante per la tutela dei dati personali del 13 ottobre 2008. In caso di impossibilità o impedimento dell'Utente, ovvero laddove lo stesso, prima della cessazione del rapporto, non abbia reso disponibili i file attinenti l'attività di servizio/collaborazione e non abbia delegato un collega a inoltrarli, il Direttore, o un suo delegato, può accedere alle risorse assegnategli per il periodo necessario a recuperare i dati di interesse. In caso di grave improvvisa indisponibilità o decesso dell'Utente, il Direttore, su richiesta, potrà rendere disponibile agli aventi diritto i file con contenuti personali.

Gli **Utenti** che hanno privilegi di amministratore sui loro sistemi (p.e. laptop) sono tenuti a prendere visione dei relativi documenti con le Norme d'uso, in attuazione della Circolare AgID 18/04/2017 n. 2/2017, e a seguirne scrupolosamente le indicazioni.

7. INDIVIDUAZIONE E COMPITI DEL REFERENTE DI GRUPPO DI UTENTI

Il Referente del gruppo di utenti è individuato dal Direttore della Struttura cui afferisce in ragione delle funzioni assegnate. Il Referente può essere altresì individuato dalla collaborazione scientifica cui appartiene. La designazione è comunicata al Servizio di Calcolo e Reti competente.

Il **Referente**:

1. divulga, nell'ambito del proprio gruppo, le indicazioni del Servizio di Calcolo e Reti relative alla sicurezza delle risorse ed al corretto uso delle stesse;
2. in caso di necessità, fornisce al Servizio di Calcolo e Reti informazioni o accesso alle risorse di calcolo del proprio gruppo.

8. INDIVIDUAZIONE E COMPITI DEGLI AMMINISTRATORI DI SISTEMA

Gli **Amministratori di Sistema** sono designati dal Direttore della Struttura di afferenza con apposito atto.

Nel caso in cui l'attività dell'Amministratore di Sistema riguardi risorse informatiche collocate presso più Strutture, l'atto di designazione è comunicato al Direttore e al Servizio di Calcolo e Reti di ciascuna Struttura.

Gli **Amministratori di sistema**, oltre all'osservanza di tutte 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. segnalare immediatamente al Servizio di Calcolo e Reti incidenti, sospetti abusi e

violazioni della sicurezza e partecipare alla loro gestione;

5. installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono;
6. non visionare i dati personali e della corrispondenza di cui dovessero venire a conoscenza e comunque a considerarli strettamente riservati e a non riferire, né duplicare o cedere a persone non autorizzate informazioni sull'esistenza o sul contenuto degli stessi;
7. in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;
8. seguire attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.

9. COMPITI DEL SERVIZIO CALCOLO E RETI

Il **Servizio Calcolo e Reti**, al fine di mantenere il più elevato livello di sicurezza all'interno delle reti locali, in relazione all'evoluzione tecnologica del settore:

1. 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;
2. limita l'uso interno di servizi e programmi che trasmettono in chiaro le password;
3. sulle macchine gestite, provvede a disattivare i servizi non essenziali ed a limitare 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;
4. effettua la revisione, almeno annuale, degli account;
5. effettua il monitoraggio della rete e dei sistemi gestiti, incluse le risorse utilizzate per l'erogazione di servizi di tipo *cloud*, al fine di garantirne la funzionalità e la sicurezza;
6. realizza i sistemi di filtraggio e logging sugli apparati perimetrali della rete;
7. fornisce supporto per conservare e incrementare la sicurezza delle risorse affidate agli utenti.

10. DISPOSIZIONI PER L'USO DEI SERVIZI ESTERNI

Il trattamento dei dati personali di qualunque tipo o di particolare rilevanza per l'Ente può essere effettuato mediante l'uso di servizi esterni, anche di tipo *cloud*, soltanto ove l'INFN 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 oltre ai profili di responsabilità nel trattamento.

11. TRATTAMENTO DEI DATI ACQUISITI IN RELAZIONE ALL'USO DELLE RISORSE DI CALCOLO E ALL'ACCESSO AI SERVIZI DI RETE

L'INFN, nel rispetto dei principi di libertà e dignità, 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 quali:

a) la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per svolgere il servizio di posta elettronica;

b) la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dall'utente;

c) la lettura e registrazione dei caratteri inseriti tramite tastiera o dispositivi analoghi;

d) l'analisi occulta di computer portatili affidati in uso.

Con riferimento all'accesso alla rete, il Servizio Calcolo e Reti, per le finalità indicate al punto successivo raccoglie le informazioni relative all'associazione tra indirizzo, nome del computer e utente; non registra il contenuto delle connessioni, può raccogliere tuttavia alcune informazioni relative alle transazioni eseguite quali: indirizzi dei nodi, ora di inizio e fine transazione e quantità dei dati trasferiti.

I dati di cui al paragrafo precedente sono conservati per un periodo non superiore a un anno e sono utilizzabili dal personale del Servizio di Calcolo e Reti competente solamente con fini di controllo della sicurezza e per l'ottimizzazione dei sistemi.

Le Strutture in cui sono installati proxy server o altri sistemi di controllo delle sessioni possono conservare i file di log contenenti informazioni relative alle pagine web, interne od esterne, accedute dai nodi locali. Tali informazioni, conservate per un periodo non superiore a sette giorni a cura del Servizio di Calcolo e Reti, sono esaminate o elaborate soltanto ove si ravvisi la necessità di garantire la sicurezza o il buon funzionamento del sistema.

12. RACCOLTA DATI IN RELAZIONE AL SERVIZIO DI POSTA ELETTRONICA

Il Servizio di Calcolo e Reti per esigenze organizzative connesse al funzionamento, sicurezza e salvaguardia del servizio di posta elettronica registra data, ora, indirizzi del mittente e del destinatario dei messaggi di posta, nonché il risultato delle analisi dei software antivirus ed antispam.

I dati registrati, utilizzati anche per elaborazioni statistiche, sono conservati per un periodo non superiore a un anno e sono accessibili dal solo personale, appositamente incaricato, del Servizio di Calcolo e Reti di competenza.

Per le medesime finalità le Strutture che effettuano copie di salvataggio dei messaggi di posta elettronica conservano tali copie per un periodo non superiore a un anno a cura del Servizio di Calcolo e Reti di competenza.

Ciascuna Struttura, ove compatibile con la propria organizzazione, può rendere disponibili indirizzi di posta elettronica condivisi attraverso l'uso di liste di distribuzione di e-mail, nonché messaggi di risposta automatica, in caso di assenza programmata dei titolari.

La casella di posta elettronica è disattivata entro i due mesi successivi alla scadenza del

termine nel quale l'utente è stato autorizzato all'accesso. Entro tale periodo l'utente ha il dovere di trasferire al Direttore o a un suo delegato le comunicazioni di servizio d'interesse e di trasmettergli quelle nel frattempo intervenute. Il contenuto della casella è comunque cancellato entro un anno dalla scadenza del termine di autorizzazione all'accesso. I periodi indicati nel presente capoverso possono essere prolungati dal Direttore ove ne ravvisi specifica esigenza.

In caso di impossibilità o impedimento del titolare della casella di posta elettronica, il Direttore o un suo delegato può avere accesso alla casella per un periodo non superiore a un mese dalla data di conoscenza della situazione che ha determinato l'impossibilità o l'impedimento.

13. 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 adotta misure che consentono la verifica di comportamenti anomali o delle condotte non previste dal presente Disciplinare nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati. A tal fine il Servizio di Calcolo e Reti può eseguire elaborazioni sui dati registrati dirette ad evidenziare anomalie nel traffico di rete o condotte non consentite dal presente Disciplinare.

Nel caso in cui, nonostante l'adozione di accorgimenti tecnici preventivi, si verifichino eventi dannosi o rilevino comportamenti anomali o non consentiti, il Servizio di Calcolo e Reti esegue, previa informazione agli interessati e salvo i casi di necessità ed urgenza, ulteriori accertamenti e adotta le misure necessarie ad interrompere le condotte dannose o non consentite.

Nei casi di reiterazione di comportamenti vietati e già segnalati o di particolare gravità, il Responsabile del Servizio di Calcolo e Reti adotta tutte le misure tecniche necessarie, dandone immediata comunicazione al Direttore di Struttura, che dispone gli ulteriori provvedimenti ai sensi del punto seguente.

I Direttori di Struttura, in relazione alle funzioni loro assegnate circa il trattamento dei dati personali, adottano ogni opportuna misura affinché i soggetti preposti al trattamento dei dati relativi all'uso di internet e della posta elettronica svolgano soltanto le operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, neppure di propria iniziativa.

14. VIOLAZIONE DELLE NORME

Ogni condotta posta in essere in violazione del presente Disciplinare potrà determinare la sospensione dell'accesso alle risorse di rete, 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, nei confronti del responsabile, l'esercizio del diritto di rivalsa nelle forme e nei limiti stabiliti dalla legge.

15. INFORMATIVA

Il presente Disciplinare costituisce informativa ai sensi dell'art. 4, c. 3, della legge 20 maggio 1970 n.300 e s.m.i. circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse di calcolo e dei servizi di rete.

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 elettroniche o cartacee, idonee comunque a dimostrare l'avvenuta consegna.

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

16. CLAUSOLA DI REVISIONE

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

CORSO BASE DI SICUREZZA INFORMATICA

Il corso si articola su 7 moduli della durata complessiva di 1h30'-2h00' incluso il tempo stimato per il test finale.
E' inoltre presente una parte di approfondimento facoltativa di 1h00' circa.

TITOLI MODULI

1. Obblighi, norme d'uso ed informazioni generali;
2. Protezione dei propri devices;
3. E-mail e navigazione web;
4. Password;
5. Protezione dei file e dei dati;
6. Copyright e file sharing;
7. Stimolo delle sensibilita' personali alle problematiche di sicurezza.

REGULATION
ON THE USE OF INFN COMPUTING RESOURCES

24 JANUARY 2020

1. General Principles

The National Institute for Nuclear Physics (INFN) is a research national public Institute governed by the provisions set forth in its statute.

INFN considers computing facilities, and network services, as well as related data and processed information, as an integral part of INFN assets and necessary to the achievement of its own institutional aims of scientific and technological research.

This regulation is meant to safeguard INFN computing systems security and to protect the privacy, integrity and availability of information and data produced, collected and anyway processed therefrom, including the personal ones.

INFN as partner of the association GARR Consortium – the Italian network of universities and research – and user of its related services and tools, in this regulation intends to ensure compliance with the rules dictated by the GARR Consortium.

INFN collects and processes data relating to the use of computing facilities and network services, only for specific, explicit and lawful purposes, in full accordance with the principles of need, relevance, correctness and non-redundancy according to the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data. Consequently information systems and software are configured so as to minimize the use of personal and identification data.

Those who are entitled to use computing facilities and network services shall comply with the rules set forth hereinafter, which define and integrate the minimal obligations of behaviour laid down in the INFN code of conduct, in addition to behaviour inspired by principles of correctness and diligence.

2. Scope

This regulation applies to those who are entitled to use INFN computing facilities and network services.

3. Definitions

The terms **computing facilities** and **network services** refer to:

- computers and similar electronic devices, printers and other devices (e.g. scanner and storage systems) belonging to the Institute or anyhow connected to its network.
- equipment and networking infrastructure belonging to the Institute or anyhow connected to the Institute's network.
- local and geographical networking service with the exception of the geographical access guaranteed by agreements between Institutions and Federations (e.g. Eduroam)
- virtual machine instances or networking equipment;
- software and data purchased, produced or published by the Institute.

In the framework of this regulation, computing facilities and network services considered as a whole can be defined as **computing resources**.

Individuals using computing resources belonging to INFN can be identified as:

- **User**: anyone who has access to INFN computing facilities and network services, according to the functions and professional duties they perform in the Institute.
- **User group contact person**: a person who coordinates the users and the usage of local computing resources belonging to one or more groups, experiments or services, in accordance with the guidelines provided by the Computing and Networking Service.
- **System administrator**: a professional who manages equipment for data processing, even personal data and including database systems, local area networks and security equipment.
- **Computing and Networking Service**: the service responsible for managing central computing facilities, both internal and external networking of each structure, as well as implementing and developing them. It provides users with assistance in accessing the resources and the network and it has also expertise on the security of every computing facility in its own Structure.
- **Director of the Structure**: the person who shall ensure the scientific, organizational and administrative operation of each Structure as defined in the provisions set forth by INFN statute, in compliance with the guidelines adopted by the Board of Directors.

4. Access to IT resources

Upon identification and according to the rules laid down in this regulation, employees and associated personnel, as well as collaborators, guests, PhDs, specializing and graduating students, grantees and anyone else authorized, are allowed to access the INFN computing resources and network services.

Access authorization is granted by the Structure Director or by his delegate for a limited period of time, not exceeding the duration of their professional duties within INFN.

Access is personal, it cannot be shared or transferred and it is allowed only in compliance with the rules of this regulation.

5. General provisions for the use of IT resources

Computing resources, as essential to INFN, are made available for the achievement of INFN institutional objectives.

Users shall make use of IT resources safeguarding their integrity and ensuring the proper functioning.

Hence, the following activities are prohibited:

a) activities that contravene the national and international law, in breach of Community legislation or are not permitted by the ordinary usage of the networks and the services provided.
b) unauthorized commercial activities, or any other profit-making activities. The transmission of commercial and/or spamming advertising material, as well as the use of its resources by third parties for such activities.
c) activities liable to damage, destroy, jeopardize the security of INFN IT resources, or aimed at breaking the privacy and/or damaging third parties, including the creation,

transmission and preservation of images, data or any other material that is offensive, obscene, defamatory, indecent or likely to undermine human dignity, especially when relevant to sex, race, religion, political opinions or personal and social condition.

d) activities in conflict with other institutional aims.

The use of IT resources for personal aims may be tolerated as long as it does not violate any applicable laws and complies with the rules of this regulation and with all the indications provided by INFN.

6. Specific provisions for the use of IT resources

In order to guarantee the security of computing facilities and networking services it is prohibited to:

1. connect computing facilities to the local network or to any services involving network connectivity without the authorization of the Computing and Networking Service;
2. wire, connect or modify network equipment without being authorized by the Computing and Networking Service;
3. use network addresses and names that have not been explicitly granted;
4. install hardware or software systems that enable access to IT resources without being authorized by the Computing and Networking Service;
5. provide access to IT resources to persons who have not been explicitly authorized;
6. disclose information on IT resources structure and configuration, especially those concerning remote access;
7. access the Computing and Networking Service areas, as well as the areas reserved for network equipment, without being authorized;
8. undertake any other action aimed at degrading system resources, preventing authorized access to resources, getting greater resources than those authorized or accessing resources by violating the security measures.

Moreover **users** shall**:**

9. act in compliance with the law and in accordance with the security directions provided by Computing and Networking Service. They are required to ensure the privacy of processed personal data by proper observance of the rules established by INFN and published on the INFN DPO website and on the dedicated websites of Computing and Networking Service of INFN Structures;
10. take into account the guidelines provided by the Computing and Networking Service related to the choice of computing devices to use, especially for what concerns their security-related features. They shall prefer systems and procedures offering the highest levels of protection;
11. be responsible for the data and for the software they install on the computers entrusted to them: they are required to examine software carefully and in advance and do not install any software with no regular licenses.
12. protect from unauthorized access data used and/or stored in the computers and systems they are allowed to access;
13. carefully evaluate the reliability of external services, including *cloud* services, in terms of security, storage and data confidentiality.
14. follow the Computing and Networking Service recommendations concerning the regular back up of data and used programmes;

15. protect their account by passwords on condition that they comply with the security rules provided by the Institute and the Computing and Networking Service and, in the event of multiple authentication systems, by using different passwords for each system.
16. not share their passwords, nor allow even occasional use by anyone other than the account holder;
17. immediately notify any incidents, suspected abuses and security breaches to their contact person and to the Computing and Networking Service.
18. use updated anti-virus software where operating systems require that. They shall take care to scan all software and files exchanged over the network and all removable media they use;
19. not maintain unused remote connections nor leave their workstation unattended with unprotected open connections.
20. be required to transfer, on the termination of the employment/collaboration relationship, the files related to their working activity/collaboration to the person responsible, or to the Director of the Structure or to the latter's delegate, and to permanently delete any other files. INFN shall provide for the complete deletion of any data related to the user, recorded on computing resources, not later than two months from the termination date of employment/collaboration relationship, in accordance with the provisions established by the Data Protection Supervisor regulation of 13 October 2008. Where the user is unable or prevented or has failed to make the files relative to his working/collaborating activities available, and neither has he delegated a colleague to forward them, prior to the termination of his said working relationship, the Director or his delegate, may access the user's resources for the necessary time to recover the relevant data. In case of death of the user or when the user is unavailable due to a serious and sudden impediment, the Director may make, upon request, the user's personal files available to those persons so entitled.

The **Users** who have privileges as administrators on their own systems (e.g. laptops), are required to read the documentation and related Regulation on the use of systems, to comply with the AgID Circular 18/04/2017 no. 2/2017 and to take all necessary measures there established.

7. Identification and tasks of the user group contact person

The user group contact person is identified by the Director of the Structure concerned. The contact person can also be identified by the scientific collaboration he/she belongs to. The Computing and networking Service concerned shall be informed on his designation.

The **user group contact person**:

1. delivers to his group any Computing and Networking Service directions concerning the security of resources and their proper use.
2. when needed, provides Computing and Networking Service with information or access to the computing facilities of his group.

8. Identification and Tasks of the System administrators

The designation of the system administrators is provided by the Director of the Structure with a specific Act.

Where the system administrator's activities concern computing resources located in more than one structure, the Act of designation shall be communicated to the Director and the Computing and Networking Service of each Structure.

System administrators, in addition to abiding by all the above-mentioned rules, shall

1. keep systems at the appropriate level of security for their use;
2. verify regularly system integrity;
3. check and maintain system logs for the time necessary to test the preservation of security standards;
4. notify immediately incidents, suspected abuses and security breaches to the Computing and Networking Service, and collaborate to handle them;
5. install and keep anti-virus software up-to-date, for operating systems that require it;
6. not inspect personal data and correspondence they become aware of and consider them as strictly confidential. They shall not report, duplicate nor transfer content and information on their existence to unauthorized persons;
7. in case of servicing or maintenance work on the systems they manage, they shall prevent as far as possible access to information and to personal data stored in the systems;
8. attend training courses in technical-managerial matters and network security, as well as in data protection and correspondence confidentiality.

9. Tasks of the Computing and Networking Service

In order to keep the highest level of security in the local networks and in relation with the technological development of its branch, the Computing and Networking Service shall:

1. verify that remote logins to the local facilities take place exclusively through the use of protocols providing authentication and encryption of the transmitted data;
2. limit the internal use of services and software sending unencrypted passwords;
3. disable non-essential services on the equipment under its jurisdiction and restrict the number of privileged users to the minimum strictly needed for performing activities of coordination, control and monitoring of the network and its related services;
4. perform the review of accounts on a yearly basis;
5. monitor the network and systems they manage, including the resources on *cloud* infrastructures, in order to ensure their effectiveness and security;
6. implement filtering and logging systems on the perimetric network devices.
7. help to preserve and increase the security of resources entrusted to users.

10. Provisions for the use of external services

The INFN may use external services, including the *cloud*, in processing personal data - whether common or sensitive – any type of data or data of particular importance for the Institute, only after checking out the risks and benefits related to the offered services, the limits on circulation and data transfer, as well as the reliability of the supplier, the existence of guarantees and precautions for storage, persistence and data confidentiality, in addition to data processing liability.

11. Processing data obtained by using computing facilities and by accessing the network

The remote control of users and related data processing achieved by installing specific hardware equipment or software, is prohibited by INFN, in compliance with the principles of freedom and dignity. In particular:

a) systematic recording and reading of e-mail messages, beyond what is necessary to carry out the e-mail service;
b) systematic reproducing and recording of web pages viewed by the user;
c) reading and registering characters entered by keyboard or similar devices;
d) unauthorized inspection of laptops entrusted to the user.

Regarding access to the network, the Computing and Networking Service matches information on the address, the computer name and its user for the purposes mentioned below; it does not record the content of connections, however it may collect some information concerning the transactions occurred such as: hub connections, start and end of timestamps of transaction and amount of data transferred.

The data referred to in the above paragraph shall be retained for a period not exceeding one year and can be used by the Computing and Networking Service staff only for security purposes and for systems optimization.

The Structures, where proxy server or other session control systems are installed, may save the log files containing information on web pages – whether internal or external - that are accessed from local computers. The Computing and Networking Service saves such information for a period not exceeding seven days; it analyses and processes it only if necessary to guarantee the security of the system and its proper operation.

12. Data collection relating to email service

The Computing and Networking Service records email messages' date, time, sender and recipient's addresses, as well as the result of antivirus and anti-spam software analysis, conducted for the needs related to the operation, security and integrity of email service.

The data recorded, which are also used for statistics, are stored for a period not exceeding one year and can be accessed only by the personnel specifically in charge of the Computing and Networking Service.

For the same purposes, Structures that back up email messages, shall keep the back up copies for a period not exceeding one year. The Computing and Networking Service is responsible for taking care of the backup.

Where compatible with its organization, each Structure can provide shared email addresses through distribution lists, as well as auto-reply messages in case of a programmed absence of the list managers.

A user's mailbox is disabled within two months following the expiry date of the period in which the user was granted access. Within this period the user is obliged to transfer any useful communications and other communications occurred meanwhile to the Director or to a delegate of theirs. In any case the mailbox content is deleted within one year from the termination date of access authorization.

Extending the periods referred to in this paragraph is at the Director's discretion, when deemed necessary.

In the event of the mailbox owner's inability or impediment, the Director or a delegate of theirs, may have access to the mailbox for a period not exceeding one month from the date when they became aware of the situation that caused such inability or impediment.

13. Further measures for protecting information systems

In order to ensure the operation, availability, optimization, security and integrity of information systems and prevent inappropriate uses, INFN adopts measures that allow to check abnormal behaviour or conduct that are not compliant with this regulation, in accordance with the above mentioned necessity, relevance, and non-redundancy principles. The Computing and Networking Service can process recorded data for the purpose of pointing out anomalies in the network traffic or conducts not permitted by this regulation.

In the event of harmful events or upon abnormal and not permitted behaviour occurring despite the adoption of precautionary technical measures, the Computing and Networking Service, unless in cases of emergency, shall inform the parties concerned and carry out any further investigations to put into effect the necessary measures aimed at stopping any harmful and unauthorized conduct.

In case of recurrence of prohibited or serious behaviours, already reported, the Computing and Networking Service manager shall adopt all the technical measures needed, informing immediately the Structure Director who shall take further actions pursuant to the following point.

The Structure Directors carrying out their functions related to data processing, may take any necessary actions to ensure that only operations strictly necessary are performed by the persons entitled to process data related to the use of internet and emails, and that the above said persons do not carry out, not even on their own-initiative, any remote control activities,.

14. Policy violation

Any infringement of the present Regulation may result in the suspension of access to computing facilities, without prejudice to any disciplinary, civil or criminal proceedings.

Where the infringement of the provisions of this regulation causes harm to third persons who are awarded damages by INFN, the latter may exercise the right to claim compensation against the person responsible, in the forms and within the limits established by law.

15. Note

This regulation provides information pursuant to Article 3 of legislative decree 20 May 1970, no.300 and Article 4, paragraph 3, of the law 20 May 1970 no. 300 and followings concerning the terms and purposes of processing personal data related to the use of computing facilities and network services.
INFN ensures that this regulation and its subsequent updates have the widest dissemination among users through its publication on the web pages of each structure, as well as by delivering it to everybody in electronic or printed mode, in any mode suitable to prove it has been delivered.

This Regulation repeals and replaces in its entirety all the previous regulations adopted on this subject.

16. Review Clause

This regulation is periodically updated according to the technological evolution and the regulations existing in this branch.