INAF ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS

DIRETTIVA PER L'UTILIZZO DELLE RISORSE INFORMATICHE DELL'ISTITUTO NAZIONALE DI ASTROFISICA

1. Principi generali

L'Istituto Nazionale di Astrofisica (INAF), istituito con il D. Lgs. n. 296 del 23 luglio 1999, è il principale Ente di Ricerca italiano per lo studio dell'Universo, riferimento nazionale ed internazionale per la ricerca nel campo dell'astrofisica e dell'astronomia.

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

Con la presente Direttiva, l'INAF definisce le regole atte a 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'INAF, aderendo all'associazione Consortium GARR - Rete italiana dell'Università e della Ricerca - e utilizzandone i relativi servizi e strumenti, assicura con la presente Direttiva la conformità delle proprie disposizioni regolamentari interne a quelle dettate dal Consortium GARR.

L'INAF effettua il trattamento dei dati raccolti in relazione all'uso delle risorse di calcolo e dei servizi di rete 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 tale 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 disposizioni di seguito esposte, che definiscono ed integrano i doveri minimi di condotta previsti nel Codice di Comportamento dell'INAF, oltre comunque a un comportamento ispirato ai principi di correttezza e diligenza.

2. Ambito di applicazione

La presente Direttiva si applica a tutti coloro cui sia consentito l'accesso alle risorse di calcolo, di *storage* ed ai servizi di rete dell'INAF.

3. Definizioni

Nell'ambito della presente Direttiva le risorse di calcolo, di *storage* ed i servizi di rete possono essere collettivamente definite **risorse informatiche**.

Per **risorse informatiche** 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;
- sistemi di *storage* locali od *in cloud*;
- 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 e/o prodotti dall'INAF.

Ai fini della presente Direttiva, si intendono per:

- **Utente**: ogni soggetto che abbia accesso alle risorse informatiche dell'INAF, 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 ICT e del SID;
- **Amministratore di sistema**: figura professionale dedicata alla gestione e alla manutenzione di sistemi 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;
- **Responsabili delle risorse informatiche della Struttura (SID della Struttura)**: il Responsabile dei Servizi Informatici individuato da ciascun Direttore di Struttura, che ha il compito di coordinare le attività degli amministratori di

sistema per soddisfare le esigenze amministrative e di ricerca. Il Responsabile potrà assumere su di sé o suggerire alla Direzione a chi affidare i seguenti incarichi:

  - il Referente nel Gruppo di Coordinamento Sistemi Informativi (**GCSI**);
  - l'Access Point Manager (**APM**) per la gestione dei collegamenti alla rete GARR;
  - il referente nel Coordinamento per i Servizi Informatrici Amministrativi (**CSIA**);

- **Servizi Informatici per il Digitale (SID)**: articolazione organizzativa della Direzione Generale dell'INAF cui compete la gestione delle risorse di calcolo amministrative e gestionali dell'Ente, i collegamenti in rete delle Strutture, nonché l'assistenza agli utenti per l'accesso alle risorse ed ai servizi comuni, il coordinamento dei servizi informatici delle Strutture avvalendosi dei referenti GCSI e CSIA;
- **ICT**: è la Sezione della Struttura tecnica della Direzione Scientifica deputata al coordinamento, alla gestione e allo sviluppo di servizi e risorse informatiche attinenti alle "*Information and Communications Technologies*" per i progetti e le attività di ricerca dell'Ente;
- **Direttore di Struttura**: il soggetto al quale, nel rispetto degli indirizzi approvati dal Consiglio di Amministrazione, compete la responsabilità di assicurare il funzionamento scientifico, organizzativo ed amministrativo di ciascuna Struttura di Ricerca come individuata nelle disposizioni dello Statuto dell'INAF e che svolge, tra l'altro, le funzioni di "*Referente Privacy*", al fine di garantire il rispetto di tutti gli obblighi previsti dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("*Regolamento Generale sulla Protezione dei Dati*" - "*RGPD*" o "*General Data Protection Regulation*" - "*GDPR*") e dalla normativa nazionale in capo all'Istituto in qualità di "*Titolare del trattamento*";
- **APA** (Access Point Administrator): soggetto incaricato dal Direttore Generale o dal Presidente dell'Ente che interagisce con la Direzione del Consortium GARR e che ha il compito di assicurare la piena e corretta funzionalità della rete locale dell'Istituto, secondo le sue specifiche linee gestionali, ed ottimizzare l'uso della Rete GARR da parte delle Strutture;
- **Data Protection Management Unit (DPMU):** Gruppo permanente presieduto dal Direttore Generale cui partecipano stabilmente il Responsabile dell'articolazione

organizzativa della Direzione Generale "*Servizi Informatici per il Digitale*" ("SID"), il Responsabile della Sezione della Struttura tecnica della Direzione Scientifica "*Information and Communication Technologies*" ("*ICT*"), il Responsabile del Servizio di Staff alla Direzione Generale "*Affari Legali, Contenzioso e Supporto Tecnico agli Organi*" ed il Responsabile della Protezione dei Dati, che ha il compito di sovraintendere allo svolgimento delle attività di trattamento di dati personali svolte dall'Istituto e di definire le misure tecniche ed organizzative volte ad assicurare il corretto adempimento delle disposizioni di cui al Regolamento (UE) 2016/679 e la concreta applicazione delle indicazioni provenienti dal Garante per la protezione dei dati personali;

- **Data Protection Local Unit (DPLU)** o **Gruppo privacy:** Unità operative in tutte le strutture di ricerca dell'Ente che hanno il compito di sovraintendere allo svolgimento delle attività di trattamento di dati personali svolte presso le Strutture stesse, al fine di supportare il Referente privacy nello svolgimento delle attività di sua competenza e di garantire il rispetto di tutti gli obblighi previsti dal Regolamento (UE) 2016/679 e dalla normativa nazionale in capo all'Istituto in qualità di "*Titolare del trattamento*";
- **Responsabile della protezione dei dati (RPD)** o ***Data Protection Officer* (DPO)**: è la figura introdotta dagli articoli 37-39 del Regolamento (UE) 2016/679, ovvero una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati personali e verifichi l'adeguatezza delle soluzioni adottate dall'Ente.

4. Accesso alle risorse informatiche

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

L'autorizzazione all'accesso ai servizi nazionali dell'INAF avviene attraverso credenziali che sono assegnate con l'iscrizione nell'anagrafica dell'Ente. L'autorizzazione all'uso delle risorse locali 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'INAF.

L'accesso è personale, non può essere condiviso o ceduto e il relativo utilizzo è consentito a ciascun utente soltanto in conformità alle disposizioni della presente Direttiva e della normativa vigente applicabile.

5. Disposizioni generali per l'utilizzo delle risorse informatiche

Le risorse informatiche, in quanto essenziali per l'INAF, sono rese disponibili per il conseguimento delle finalità istituzionali dell'Ente.

Gli utenti sono tenuti a servirsi delle risorse informatiche dall'Ente loro assegnate in dotazione prestando il proprio contributo affinché ne sia preservata l'integrità e garantito il buon funzionamento.

Sono pertanto vietate:

a) attività contrarie alla legge nazionale, comunitaria e internazionale o proibite dai regolamenti delle reti e dei servizi acceduti;
b) 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;
c) 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;
d) attività comunque non conformi ai fini istituzionali dell'Ente.

E' consentito l'utilizzo delle risorse informatiche per finalità personali purché questo non violi le leggi applicabili e sia compatibile con le disposizioni della presente Direttiva, e successive modifiche ed integrazioni, nonché dai vigenti regolamenti e disciplinari dell'Istituto.

6. Disposizioni specifiche per l'utilizzo delle risorse informatiche

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

a) connettere risorse informatiche alla rete locale o ad altri servizi che includono la connettività di rete senza l'autorizzazione del Responsabile delle risorse informatiche;
b) cablare, collegare o modificare apparati di rete senza l'autorizzazione dell'APM;
c) utilizzare indirizzi di rete e nomi non espressamente assegnati;
d) installare sistemi, hardware o software, che consentano accesso alle risorse informatiche senza l'autorizzazione del Responsabile;
e) fornire accesso alle risorse informatiche a soggetti non espressamente autorizzati;
f) divulgare informazioni sulla struttura e configurazione delle risorse informatiche, con particolare riferimento a quelle che consentono accesso da remoto (VPN, firewall);
g) accedere senza autorizzazione ai locali dei servizi di calcolo, nonché ai locali ed alle aree riservate alle apparecchiature di rete;
h) 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:

a) sono tenuti ad agire in conformità alla legge e nel rispetto delle indicazioni del RPD - Responsabile della Protezione dei Dati in materia di sicurezza, garantendo la riservatezza nel trattamento dei dati personali;
b) nella scelta degli strumenti informatici di cui si servono, devono tenere in opportuna considerazione le indicazioni del SID - Servizi Informatici per il Digitale e dell'ICT - *Information and Communications Technologies*, in particolare per quanto riguarda le caratteristiche relative alla sicurezza, privilegiando i sistemi e le procedure che offrono i livelli più elevati di protezione;
c) 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;
d) sono tenuti a proteggere da accessi non autorizzati i dati utilizzati e/o memorizzati nei propri computer e nei sistemi cui hanno accesso;

e) valutano attentamente l'affidabilità dei servizi esterni eventualmente utilizzati, ivi inclusi quelli di tipo *cloud*, in termini di sicurezza, conservazione e confidenzialità dei dati;
f) sono tenuti a proteggere il proprio account mediante password non banali e, qualora siano presenti più sistemi di autenticazione, differenti per ogni sistema;
g) non devono diffondere né comunicare la propria password, ovvero concedere ad altri l'uso del proprio account;
h) sono tenuti a segnalare immediatamente al responsabile informatico della struttura incidenti, sospetti abusi e violazioni della sicurezza. Qualora vi sia il sospetto di accesso o violazione dei dati personali, va immediatamente informata la DPLU della struttura;
i) 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;
j) qualora operino su computer condivisi o in uffici condivisi non devono mantenere connessioni remote inutilizzate né lasciare la postazione di lavoro con connessioni aperte non protette;
k) non devono riprodurre o duplicare materiale coperto da copyright.

7. Compiti degli Amministratori di sistema

Gli **Amministratori di sistema**, oltre all'osservanza di tutte le disposizioni precedenti, sono tenuti a:

a) mantenere i sistemi al livello di sicurezza appropriato al loro uso;
b) verificare con regolarità l'integrità dei sistemi;
c) controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;
d) segnalare immediatamente al Responsabile informatico della struttura sospetti abusi e violazioni della sicurezza e partecipare alla loro gestione. Qualora vi sia il sospetto di accesso o violazione dei dati personali (c.d. "*Data breach*"), va immediatamente informata la DPLU della struttura;
e) installare e mantenere aggiornati programmi antivirus per i sistemi che lo prevedono;

f) 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;
g) in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;
h) seguire e stimolare attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.

8. Compiti del Responsabile SID di Struttura

Il responsabile, con la collaborazione degli amministratori di sistema, al fine di mantenere il più elevato livello di sicurezza all'interno delle reti locali, in relazione all'evoluzione tecnologica del settore:

a) 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;
b) si accerta che le password di amministrazione degli apparati che garantiscono la funzionalità e l'operabilità dei servizi della struttura siano condivise da almeno due amministratori di sistema e mantiene aggiornato un elenco che sarà conservato in busta chiusa presso la Direzione della struttura;
c) limita l'uso interno di servizi e programmi che trasmettono in chiaro le password;
d) 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;
e) effettua la revisione, almeno annuale, degli account;
f) effettua il monitoraggio dei sistemi gestiti, registrando gli accessi privilegiati, eventuali modifiche ai file di sistema e l'uso non autorizzato dei servizi di rete;
g) realizza i sistemi di filtraggio e logging sugli apparati perimetrali della rete in collaborazione con l'APM;
h) fornisce supporto per conservare e incrementare la sicurezza delle risorse affidate agli utenti;

i) verifica l'aggiornamento degli indirizzi telefonici e di posta elettronica degli APM e dell'APA sul sito del GARR;
j) segnala alla Direzione della struttura situazioni che possano mettere a rischio la sicurezza dell'infrastruttura informatica o comportamenti che contravvengono la presente Direttiva;
k) segnala immediatamente alla DPLU qualunque evento che possa prefigurarsi come "*Data breach*" o sospetta violazione dei dati personali;
l) dà idonea diffusione alla presente Direttiva, eventualmente integrandola con specifiche regole locali.

9. Referenti GCSI, CSIA e APM

Per un uso coordinato delle infrastrutture, delle risorse e dei servizi informatici e di rete da parte delle Strutture, per mantenere un rapporto con i Servizi e gli Uffici nazionali dell'INAF sono state individuate le figure di referenti CGSI e CSIA e di APM.
A seconda dell'assetto organizzativo di ciascuna Struttura, gli incarichi potranno essere conferiti al Responsabile del SID della struttura od affidati ad altri dipendenti; è tuttavia auspicabile che la funzione di referente GCSI sia assunta dal Responsabile SID locale.

Il **Referente GCSI di Struttura**:

a) partecipa agli incontri per il coordinamento dell'infrastruttura informatica dell'Ente;
b) divulga, nell'ambito del propria Struttura, le indicazioni dei servizi SID e del ICT relative alla sicurezza delle risorse ed al corretto uso delle stesse;
c) in caso di necessità, fornisce al SID e all'ICT informazioni o accesso alle risorse di calcolo della propria struttura.

Il **Referente APM di Struttura**:

a) collabora con i tecnici del GARR ed in particolare con il GARR-CERT per la risoluzione dei problemi relativi alla sicurezza di rete che vengono segnalati, informando celermente il SID e l'ICT per i problemi rilevati;
b) fa riferimento all'APA (Access Port Administrator) dell'INAF nei casi in cui siano richiesti interventi che coinvolgono diverse Strutture dell'Istituto o altri Enti ed organizzazioni che utilizzano la rete GARR.

Il **Referente CSIA di Struttura**:

a) divulga, nell'ambito del propria Struttura, le indicazioni dei servizi SID relative alla sicurezza delle risorse informatiche degli uffici amministrativi ed al corretto uso delle stesse;
b) applica le "misure minime di sicurezza" previste dall'Agenzia per l'Italia Digitale (AgID) alle risorse informatiche degli uffici amministrativi ed ogni altra misura di sicurezza ritenuta adeguata;
c) in caso di necessità, fornisce al Responsabile del SID nazionale informazioni o accesso alle risorse di calcolo della propria struttura;
d) predispone le informative per la DPLU nel caso di infrazione ai sistemi che hanno comportato violazioni di dati personali.

10. Disposizioni per l'utilizzo dei servizi esterni

Il trattamento dei dati personali, sia comuni che sensibili, o di particolare rilevanza per l'Ente può essere effettuato mediante l'uso di servizi esterni, anche di tipo *cloud*, nel rispetto delle indicazioni fornite da AgID per le applicazioni amministrative e gestionali e previa verifica dei rischi e dei benefici connessi ai servizi offerti, dei limiti nella circolazione e trasferimento dei dati, nonché dell'affidabilità del fornitore, della sussistenza di garanzie e cautele per la conservazione, persistenza e confidenzialità dei dati oltre ai profili di responsabilità nel trattamento secondo quanto stabilisce il GDPR.

Rimarrà in capo al singolo utente la responsabilità dell'utilizzo di servizi esterni che vengono utilizzati per fini di ricerca. Anche se l'accesso a tali servizi è stato acquisito dall'Ente, l'utente risponderà individualmente dell'uso che viene fatto delle singole applicazioni da lui utilizzate.

11. Trattamento dei dati acquisiti in relazione all'utilizzo delle risorse informatiche e all'accesso ai servizi di rete

L'INAF, 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 dei messaggi di posta elettronica, al di là di quanto necessario per svolgere il servizio;

b) la riproduzione ed eventuale memorizzazione 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, per le finalità indicate al punto successivo raccoglie le informazioni relative all'associazione tra indirizzo, nome del computer e utente.

Il Servizio può acquisire informazioni relative agli indirizzi dei nodi, orario di inizio e fine della trasmissioni e quantità di dati trasferiti, ma non può in nessun caso registrare il contenuto delle trasmissioni effettuate. I dati saranno conservati per un periodo non superiore a un anno e saranno utilizzabili dagli amministratori di sistema esclusivamente per finalità 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 degli amministratori di sistema, sono esaminate o elaborate soltanto ove si ravvisi la necessità di garantire la sicurezza o il buon funzionamento del sistema.

La conservazione di log o di altre informazioni per periodi superiori a quanto indicato per fini di analisi statistica deve prevedere la pseudonimizzazione degli indirizzi.

12. Servizio di posta elettronica

L'INAF fornisce a dipendenti e collaboratori caselle di posta elettronica che devono essere utilizzate per le finalità istituzionali dell'Ente. Non è vietato, ma va scoraggiato, l'uso della casella postale istituzionale per le comunicazioni private, anche considerando che l'accesso a tutti i servizi informatici dell'Ente cessa dopo 6 mesi dalla scadenza del rapporto.

L'INAF ha esternalizzato il servizio di posta elettronica per gli utenti, ma mantiene comunque alcuni server attivi per esigenze particolari. L'assegnazione delle caselle postali presso l'operatore esterno avviene in via automatica, a partire dall'anagrafica dell'Ente, e la gestione è in carico alle singole Strutture. Le caselle postali sui server dell'Ente sono gestite dagli amministratori di sistema della struttura.

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.
Tutti i servizi digitali e la casella di posta elettronica rimarranno attivi per ulteriori sei mesi dalla scadenza del rapporto con l'Ente. Entro tale periodo l'utente ha il dovere di cancellare tutte le mail personali trasferendo al Direttore, o a un suo delegato, le comunicazioni ed i file che reputa di interesse per l'Ente. Come previsto dal contratto con il fornitore del servizio l'utenza, la casella di posta elettronica e i dati nelle aree *cloud* saranno cancellati definitivamente entro i sei mesi successivi.
I server di posta elettronica attivi presso le strutture applicheranno una analoga politica di conservazione.
Con particolare riferimento ai server postali che rimarranno attivi nell'Ente, gli amministratori di sistema, 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 incaricato dal Responsabile SID della struttura.
Le Strutture che effettuano copie di salvataggio dei messaggi di posta elettronica conservano tali copie per un periodo non superiore a sei mesi.
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. Cessazioni delle utenze e riconsegna dei dispositivi

Alla cessazione del rapporto con l'Ente, sarà cura dell'utente salvare su propri dispositivi eventuali file personali presenti nei sistemi di *storage* dell'INAF, considerando anche quelli ospitati su servizi *in cloud* acquisiti dall'Ente.
Tutti i dispositivi informatici di uso personale (PC, portatili, tablet, smartphone) dati in affidamento dovranno essere riconsegnati prima della cessazione del rapporto e saranno ricondizionati riportandoli alle condizioni originali.

L'utente potrà mantenere le credenziali per accedere ai servizi nazionali INAF e ai dati di sua proprietà per un periodo di 6 mesi, provvedendo, entro tale periodo, a eliminare tutti i file personali e a segnalare l'esistenza di materiale di possibile interesse per il gruppo di lavoro.
Al termine di tale periodo l'utenza sarà disabilitata ed eventuali richieste di accesso ai dati dovranno essere indirizzate al Direttore della Struttura o al Referente del proprio gruppo di lavoro. A sei mesi dalla cessazione del rapporto, tutti i dati di proprietà dell'utente dovranno essere eliminati a cura degli Amministratori di sistema.

14. Smaltimento dei dispositivi di memorizzazione

Al fine di evitare che dati sensibili o personali, oppure credenziali di accesso memorizzate possano essere recuperate da materiale dismesso e smaltito dall'Ente, gli Amministratori di sistema devono provvedere a cancellare i supporti magnetici e a formattare tutti i dispositivi (smartphone, tablet, portatili … chiavette USB) prima dello smaltimento degli stessi.
Nel caso di supporti di memorizzazione che hanno contenuto dati personali o di dispositivi non più funzionanti, e che quindi non possono essere inizializzati, è buona norma assicurarsi di mettere completamente fuori uso dischi e memorie anche ricorrendo all'uso di mezzi fisici.

15. 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'INAF adotta misure che consentono la verifica di comportamenti anomali o delle condotte non previste dalla presente Direttiva nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati.
A tal fine, l'APM può eseguire elaborazioni sui dati registrati dirette ad evidenziare anomalie nel traffico di rete o condotte non consentite dalla presente Direttiva.
Nel caso in cui, nonostante l'adozione di accorgimenti tecnici preventivi, si verifichino eventi dannosi o rilevino comportamenti anomali o non consentiti, il Responsabile SID della Struttura 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.

Nel caso in cui gli eventi dannosi comportino l'accesso non autorizzato a dati personali, il referente CSIA dovrà darne immediata comunicazione al Direttore della Struttura ed al RPD.
Nei casi di reiterazione di comportamenti vietati e già segnalati o di particolare gravità, il Responsabile del SID della Struttura adotta tutte le misure tecniche necessarie, dandone immediata comunicazione al Direttore di Struttura ed al responsabile dei Servizi Informatici per il Digitale che dispone gli ulteriori provvedimenti ai sensi del punto seguente.

16. Violazioni

Ogni condotta posta in essere in violazione della presente Direttiva determinerà la sospensione dell'accesso alle risorse informatiche, salvo eventuali azioni disciplinari, civili o penali.

17. Informativa

La presente Direttiva costituisce informativa ai sensi delle disposizioni di cui al Capo III del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("Regolamento Generale sulla Protezione dei Dati" - "RGPD" o "General Data Protection Regulation" - "GDPR") circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse di calcolo e dei servizi di rete.
L'INAF assicura alla presente Direttiva, e ai suoi successivi aggiornamenti, la più ampia diffusione presso gli utenti mediante pubblicazione nella pagina web del SID ed ICT, nonché consegnandola a ciascuno in modalità elettroniche o cartacee, idonee comunque a dimostrare l'avvenuta consegna.
Ogni Struttura è invitata a produrre guide informative, indirizzate agli Utenti, sull'utilizzo delle risorse informatiche presenti localmente. Tale documentazione dovrà essere conforme a quanto esposto nella presente Direttiva e farvi riferimento con un link esplicito.
La presente Direttiva abroga e sostituisce integralmente tutti i precedenti regolamenti adottati in materia.

18. Clausola di revisione

La presente Direttiva è aggiornata periodicamente in relazione all'evoluzione della tecnologia e della normativa di settore.