LINEE GUIDA PER L'UTILIZZO DEGLI STRUMENTI ELETTRONICI DELL'ISTITUTO NAZIONALE PER LA PROMOZIONE DELLA SALUTE DELLE POPOLAZIONI MIGRANTI E PER IL CONTRASTO DELLE MALATTIE DELLA POVERTÀ – INMP

Release V 1.0

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

Indice del documento

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

1. LINEE GUIDA PER L'USO DEGLI STRUMENTI ELETTRONICI DELL'INMP

1.1. Responsabilità degli utenti

Il sistema informatico è di proprietà dell'Istituto e può essere utilizzato dal Personale solo per scopi autorizzati e con modalità appropriate. Agli utenti viene consentito l'accesso al sistema informatico per lo svolgimento delle loro attività lavorative; essi hanno la responsabilità di utilizzare gli strumenti elettronici messi loro a disposizione in maniera corretta professionalmente, eticamente e legalmente. Consapevoli del fatto che qualunque gestore o fornitore esterno di servizi informatici potrebbe usare strumenti automatizzati per monitorare il materiale creato, memorizzato, inviato o ricevuto sulla propria rete informatica, nell'uso o accesso alle risorse informatiche dell'Istituto gli utenti devono attenersi alle disposizioni contenute nel presente documento.

Materiale inappropriato o illegale
Il materiale illegale o non appropriato, non può essere inviato per posta elettronica o con qualsiasi altra forma di comunicazione elettronica (quali ad esempio blog, reti sociali, gruppi di chat, newsgroup, etc.), né visualizzato o memorizzato sui computer dell'Istituto. Gli utenti che dovessero ricevere questo tipo di materiale devono riferire alla UOS Sistema Informativo e Statistico.
Nel caso in cui navigando in Internet si dovesse trovare materiale inappropriato è opportuno abbandonare immediatamente il sito.

Usi impropri del sistema informatico
Il sistema informatico dell'Istituto non può essere utilizzato per la diffusione o la memorizzazione di inserzioni commerciali o personali, petizioni, pubblicità, programmi distruttivi (come virus o codice auto replicante) o per qualsiasi altro uso non autorizzato.

Rispetto di leggi e licenze
Gli utenti non possono copiare illegalmente materiale protetto da copyright o da diritto d'autore o rendere questo materiale disponibile ad altri per la copia. Gli utenti sono responsabili per il rispetto delle leggi sul copyright e sul diritto d'autore, nonché per le licenze applicabili a software, file, documenti, messaggi e qualsiasi altro materiale che si desidera scaricare o copiare.

Dispendio di risorse informatiche
Gli utenti non devono deliberatamente porre in essere azioni che comportino il dispendio di risorse informatiche, ovvero la monopolizzazione ingiustificata delle stesse a danno di altri utenti. A titolo di esempio, gli utenti non devono:

- inviare grandi quantità di posta elettronica o partecipare a catene di e-mail;
- utilizzare la "navigazione" in Internet per prendere parte a gruppi di chat on line (non di lavoro) o per attività che implichino lunghi periodi di impegno di risorse senza giustificato motivo;
- stampare senza necessità lavorativa grandi quantità di documenti;
- creare in qualunque modo traffico di rete non necessario.

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

1.2. Protezione contro furti e danneggiamenti

Gli strumenti elettronici devono essere protetti con password per evitare l'accesso non autorizzato sugli stessi.
Gli utenti pertanto devono sempre accertarsi che la password di protezione sia attivata quando lasciano incustoditi gli strumenti elettronici.
Tutti i dispositivi portatili (computer, tablet, smartphone, etc.) devono essere custoditi in luoghi chiusi a chiave o comunque sicuri, al fine di evitarne il furto. Quando tali dispositivi sono utilizzati fuori dalla sede dell'Istituto, devono essere prese tutte le precauzioni utili ad evitare il furto degli stesso ovvero dei dati in essi presenti.
Il materiale cartaceo contenente dati particolari o riservati di proprietà dell'Istituto deve altresì essere custodito e protetto in armadi chiusi a chiave e accessibili solo al personale autorizzato.
L'utente deve informare subito i propri responsabili/referenti su qualsiasi danno cagionato su hardware, software e/o informazioni contenute del dispositivo.
In caso di furto o smarrimento del dispositivo mobile, il dipendente deve dare tempestiva comunicazione alla UOS Sistema Informativo e Statistico, con la presentazione della denuncia effettuata all'Autorità di pubblica sicurezza.

1.3. Riservatezza e protezione del sistema e dei dati

Tutti gli utenti sono tenuti a garantire la riservatezza dei dati dell'Istituto sui quali operano; gli nessuno di essi utente privo di autorizzazione può leggere o alterare le e-mail o le informazioni salvate su computer altrui. È vietato fare copie non autorizzate di dati dell'Istituto o divulgare a terzi informazioni se non autorizzati.
Apparecchiature, informazioni o software di proprietà dell'Istituto non devono essere portati all'esterno senza preventiva autorizzazione. L'utente non è autorizzato ad accedere, né a tentare l'accesso, alle informazioni alle quali non ha normalmente privilegi di accesso; viceversa l'utente, se per errore o a causa di un errato funzionamento del sistema, ottenesse l'accesso a funzioni o informazioni normalmente non consentitegli, dovrà immediatamente chiudere il programma o il file nel quale è entrato e informare l'UOS Sistema Informativo e Statistico. È proibita ogni attività finalizzata a violare o a sollecitare la sicurezza del sistema.
Gli amministratori, utenti privilegiati che devono assicurare il corretto funzionamento e la sicurezza della rete, dei sistemi, delle basi di dati e delle applicazioni, sono obbligati a rispettare la totale riservatezza delle informazioni alle quali hanno accesso e non possono utilizzarle né divulgarle tali.
In relazione alla normativa sulla criminalità informatica, in caso di richiesta da parte dell'Autorità Giudiziaria, l'Istituto metterà prontamente a disposizione tutte le informazioni in suo possesso, mantenendo totale riservatezza verso terzi sia dell'avvenuta richiesta sia delle informazioni messe a disposizione, come previsto dalla legge.

1.4. Regole di Clear Desk e Clear Screen

Al fine di ridurre il rischio di accesso non autorizzato alle informazioni dell'Istituto, è necessario che l'utente presti particolare attenzione a materiale cartaceo, dispositivi di memoria rimovibili e schermate video contenenti informazioni non pubbliche. Di conseguenza, l'utente dovrà aver cura di distruggere o immagazzinare in luoghi sicuri stampe, dispositivi di memorizzazioni rimovibili, file su cartelle condivise e simili. Particolare attenzione va posta alle stampe che, a volte, possono essere dimenticate sulle stampanti o ritirate dopo un tempo piuttosto lungo, lasciandole così incustodite e a disposizione di chiunque.
Anche le visualizzazioni a video possono contenere informazioni non pubbliche ed è quindi opportuno che tali schermate siano mantenute solo per il tempo strettamente necessario.

1.5. Integrità e disponibilità dei dati (Server Documentali)

L'integrità, la disponibilità, la riservatezza e la resilienza dei dati dell'Istituto è garantita quando essi vengono trattati e memorizzati sulle applicazioni messe a disposizione di tutti gli utenti. L'utente è tenuto a trasferire tempestivamente

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

sulle cartelle del server documentale i dati considerati importanti o critici per l'Istituto eventualmente presenti localmente sul proprio PC. È vietata la creazione di cartelle condivise sui PC. Eventuali dati memorizzati esclusivamente sulle postazioni di lavoro individuali non sono soggetti ad alcuna forma di protezione o salvataggio in caso di malfunzionamento, errore accidentale o manomissione.

1.6. Credenziali di accesso

In generale si ricorda che è necessario adottare un comportamento di riservatezza per tutte quelle informazioni che consentono di accedere a risorse informatiche. L'identità dell'utente è verificata attraverso lo "user-id" e la password a lui assegnate, e tutte le attività svolte da un determinato *user-id* saranno attribuite al relativo utente. Pertanto è di fondamentale importanza, ai fini della propria responsabilità, che l'utente tuteli le credenziali di accesso contro l'indebita divulgazione.
Non è consentito comunicare le credenziali di autenticazione (password, pin, …), trascriverle su biglietti facilmente rinvenibili e condividerle con altre persone. Analogamente, va protetta qualsiasi altra informazione od oggetto che abiliti all'accesso a risorse informatiche: smart card, chiavi per la firma digitale, etc.
Gli utenti sono sempre responsabili per le transazioni eseguite utilizzando le loro password o chiavi di accesso. È vietato accedere al sistema informatico utilizzando le chiavi di accesso o l'account di qualcun altro. Gli utenti non possono mascherare la loro identità mentre utilizzano il sistema informatico.

1.7. Regole d'uso delle postazioni di lavoro

L'uso delle Postazioni di Lavoro (PdL) è consentito esclusivamente per scopi istituzionali. Non è consentito installare, eseguire o scaricare qualsiasi tipo di software senza una preventiva autorizzazione da parte della UOS Sistema Informativo e Statistico.
Non è consentito riprodurre, tradurre, adattare, trasformare, distribuire software in licenza d'uso dell'Istituto.
È vietato memorizzare, utilizzare o installare strumenti hardware o software atti ad intercettare, falsificare, alterare il contenuto di documenti informatici.
Non è consentito modificare autonomamente le configurazioni impostate sulla propria postazione di lavoro, né installare sulla stessa mezzi di comunicazione propri (ad esempio chiavette per l'accesso ad Internet tramite rete mobile).
Non è consentito trasmettere, ricevere, scaricare, stampare o diffondere in qualunque modo contenuti di carattere indecente, osceno, razzista, sessualmente esplicito, illegale, immorale.
La password e gli strumenti di identificazione/autenticazione (smart card, badge, etc.) sono strettamente personali e non devono mai, per nessun motivo, essere ceduti o comunicati a terzi. La password deve essere lunga almeno 14 caratteri, di cui:

- almeno 1 maiuscolo;
- almeno 1 minuscolo;
- almeno 1 numerico;
- almeno 1 carattere speciale ($, !, &, £, %).

Qualora l'utente abbia il dubbio che le proprie credenziali di accesso siano state violate, o abbia smarrito o gli sia stato rubato il dispositivo preposto per la memorizzazione delle stesse, egli ha l'obbligo di segnalare immediatamente l'accaduto alla UOS Sistema Informativo e Statistico.
Ogni personal computer deve avere installato il software antivirus, correttamente configurato ed aggiornato; è vietato disabilitare o inibire il corretto funzionamento del software anti-virus.
Non è consentito condividere in rete file, stampanti, cartelle e altre risorse, se non attraverso gli strumenti ufficiali messi a disposizione dall'Istituto.
Ogni computer alla fine della giornata lavorativa deve essere spento, salvo giustificato motivo.

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

La PdL non deve essere lasciata incustodita durante una sessione di lavoro. Anche in caso di breve assenza il computer deve essere bloccato tramite le funzionalità offerte dal sistema (es. “blocca computer” tramite pressione contemporanea dei tasti <Ctrl+Alt+Canc> o dei tasti <logo Windows + L>).
I supporti di memoria rimovibili (chiavi USB, dischi esterni, CD, DVD, etc.) contenenti dati personali, particolari o giudiziari, devono essere conservati in luoghi protetti (ad esempio, armadi e cassettiere chiusi a chiave), cancellati quando i dati non sono più necessari, o distrutti nel caso non fosse possibile cancellarli. È sempre necessario verificare il contenuto informativo dei supporti di memoria prima della loro consegna a terzi e prima della loro eliminazione/distruzione. I file ottenuti da fonti esterne all’Istituto (file su memorie esterne, file scaricati da Internet, da reti sociali, blog o da altri servizi online, file allegati alla posta elettronica, file forniti da utenti esterni) possono contenere pericolosi virus informatici con grave rischio e danno per il regolare esercizio della rete e dei sistemi informatici dell’Istituto. Gli utenti, quindi, non devono mai scaricare file da Internet sospetti, accettare file “non sicuri” allegati alla posta elettronica o usare memorie esterne provenienti da fonti non dell’Istituto, senza prima verificare il materiale con un software antivirus approvato dalla UOS Sistema Informativo e Statistico. È buona regola cancellare tutti i messaggi e-mail di provenienza dubbia, senza “aprire” eventuali allegati.
Tutte le suddette regole valgono anche per i PC portatili e i dispositivi mobili dei Fornitori che si collegano alla rete dell’Istituto. È fatto obbligo, per i fornitori, mantenere i computer sempre aggiornati sia dal punto di vista dei miglioramenti di sicurezza che della protezione antivirus.

1.8. Regole d’uso dei dispositivi mobili

Per i dispositivi mobili utilizzati per connettersi alla rete dell’Istituto valgono le stesse regole descritte nel paragrafo precedente, ai quali si aggiungono le seguenti indicazioni specifiche legate alle caratteristiche intrinseche di questi strumenti:

- bloccare sempre il dispositivo mobile con una password;
- configurare opportunamente il blocco automatico dello schermo;
- utilizzare la crittografia dei dati (almeno nei casi in cui si trattano dati personali, particolari o giudiziari o
- riservati);
- non scaricare applicazioni da fonti non fidate;
- controllare le autorizzazioni richieste dalle applicazioni (diffidare di app che richiedono l’accesso a funzioni di
- sistema non congruenti con gli scopi dell’app stessa);
- mantenere il sistema operativo sempre aggiornato;
- diffidare di qualsiasi link si riceve da sconosciuti, via e-mail o sms o messaggi veicolati da app;
- non lasciare la connessione wi-fi sempre attiva;
- spegnere Bluetooth e NFC quando non è in uso;
- installare il software di sicurezza individuato dall’Istituto.

In caso di riassegnazione del dispositivo mobile a un altro dipendente, oppure di dismissione, deve essere realizzata la cancellazione delle informazioni presenti sul dispositivo.

1.9. Regole per l’installazione di applicazioni

L’utente di una PdL dovrà chiedere all’UOS Sistema Informativo e Statistico l’autorizzazione a installare ulteriori programmi o aggiornare le versioni esistenti. L’UOS Sistema Informativo e Statistico provvederà all’installazione o all’aggiornamento del software richiesto, dopo la verifica di liceità.
In caso di dispositivo mobile, il dipendente dell’Istituto in possesso di tale strumento, potrà installare soltanto applicazioni provenienti dai siti ufficiali dei fornitori dei dispositivi mobili (es. Galaxy Store, Windows Store, Google Play, Apple Itunes, …) e autorizzati dall’UOS Sistema Informativo e Statistico. Sono vietate tutte le applicazioni il cui

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

utilizzo può arrecare danni di reputazione oppure economici all'Istituto, nonché l'uso di programmi che violino la normativa nazionale e internazionale.

1.10. End User Computing

Di norma le applicazioni utilizzate sono fornite dall'Istituto. In alcuni casi, per valide ragioni, l'utente potrebbe avere basato le proprie necessità elaborative anche su strumenti "sviluppati localmente". Tali strumenti possono essere, ad esempio, personalizzazioni fatte su strumenti di *office automation* quali fogli *Excel*. Nel seguito essi saranno definiti come End-User Computing.
Tutte le tipologie di elaborazione appena descritte devono essere gestite in modo tale da garantire la riservatezza, l'integrità, la disponibilità e la resilienza delle informazioni. È fondamentale che l'utente comunichi per tempo alla UOS Sistema Informativo e Statistico l'esistenza di tali applicazioni in modo che questi possa attivarsi per garantire almeno i seguenti requisiti:

- esistenza di sufficiente documentazione;
- garanzia di backup e della possibilità di ripristino;
- valutazione dei rischi legati all'utilizzo di tali applicazioni;
- controllo della responsabilità di tali applicazioni;
- controllo dell'utilizzo, degli aggiornamenti e di eventuali vincoli di tali applicazioni.

1.11. Internet

L'Istituto mette a disposizione del dipendente la connessione ad Internet ai fini dello svolgimento dell'attività lavorativa.
In via eccezionale l'Istituto ammette che tale connessione venga utilizzata anche per scopi non immediatamente correlati alla prestazione lavorativa, purché ciò avvenga nel rispetto dei principi di ragionevolezza e di buona fede, evitando di mettere a repentaglio la riservatezza dei dati e delle informazioni, l'integrità del sistema informatico dell'Istituto oltre che determinare un danno all'immagine dell'Istituto. A tal fine, fermo il rispetto delle disposizioni di legge in materia e del Codice di comportamento dell'Istituto, il lavoratore non può utilizzare l'accesso ad Internet per motivi personali, se non in maniera breve ed occasionale ed in ogni caso con modalità che non arrechino intralcio o rallentamento alla normale attività lavorativa propria e di terzi.
Non è consentito lo scambio di materiale audiovisivo, cinematografico, fotografico, informatico, etc, protetto da copyright, anche se non a scopo di lucro.
Non è consentito l'utilizzo della connessione ad Internet e, più in generale, delle connessioni di rete disponibili, per l'accesso a sistemi per i quali non si è autorizzati.
È proibito l'uso del web per trasmettere o diffondere informazioni che possano danneggiare o arrecare pregiudizio all'immagine dell'Istituto ovvero che diano un'immagine non positiva dell'Istituto.
È proibita altresì qualsiasi attività (di trasmissione / download / salvataggio / connessione) illegale, fraudolenta, spiacevole, di disturbo, offensiva, discriminatoria, diffamatoria, inclusa la connessione a siti pornografici o osceni.
Allo scopo di tutelare i propri sistemi informatici, l'Istituto adotta misure di protezione del traffico Internet, anche mediante sistemi finalizzati al blocco dell'accesso a determinati siti o contenuti. È vietato aggirare o tentare di aggirare tali controlli.
Pertanto, all'utente dei servizi Internet non è consentito:

- effettuare *tunneling* http o *connect* mediante SSL;
- memorizzare le password di accesso a particolari siti web nel *browser* Internet. Le *password* non devono essere salvate nella *cache*, ma digitate ogni volta che sono richieste;

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

- utilizzare i servizi forniti dall'Istituto per effettuare attività che possano provocare malfunzionamenti, arrecare danni ad altri utenti o configurare abusi o illeciti, causare la riduzione di efficienza del servizio o arrecare danni, anche di immagine, o economica, all'Istituto, ad altri utenti e/o a terzi;
- scaricare da Internet sulla propria Postazione di Lavoro:
  - software, file e qualsiasi tipologia di materiale multimediale che viola o per mezzo dei quali possono essere violati diritti d'autore;
  - file di qualsiasi genere di dimensioni eccessive, in quanto questo può provocare un traffico elevato ed un conseguente rallentamento del servizio;
  - *cookie* che permettano di effettuare il login automatico ad un determinato sito web;
- visitare siti e/o memorizzare documenti che abbiano un contenuto contrario a norme di legge, all'ordine pubblico o al buon costume;
- accedere attraverso le infrastrutture dell'Istituto, a qualsivoglia gruppo di discussione, forum, o conferenza in rete non attinenti a questioni lavorative;
- esprimere opinioni su Internet, sfruttando il nome e i dati dell'Istituto ed utilizzando il dominio registrato dallo stesso.

All'utente del servizio Internet è richiesto di attenersi, in particolare, alle seguenti indicazioni:

- porre la massima attenzione al fine di evitare che, anche a propria insaputa, il sistema informatico sia attaccato da programmi idonei, o potenzialmente idonei, a danneggiarlo (per esempio, virus, trojan horses, cryptolocker, malware, …);
- dare comunicazione immediata all'UOS Sistema Informativo e Statistico di una sospetta vulnerabilità o di un comportamento anomalo nel funzionamento del servizio di accesso ad Internet o di altri problemi di sicurezza che dovessero sorgere in connessione alla propria attività di navigazione su Internet.

1.11.1. Accesso a servizi su cloud pubblici

L'utilizzo di servizi su cloud pubblici, quali i repository documentali come OneDrive, DropBox, GoogleDrive, iCloud etc. non è permesso, a causa delle contromisure di sicurezza delle informazioni messe in campo per proteggere il patrimonio informativo dell'Istituto. I documenti contenenti dati personali, particolari, giudiziari e, più in generale, riservati per l'Istituto, non devono mai essere salvati su questo tipo di repository in cloud.

1.11.2. Accesso ad Internet tramite connessioni esterne

È vietato connettersi a Internet avvalendosi di strumenti di connessione esterna quali chiavette Internet, router, meccanismi di Tethering attraverso un apparato mobile etc., nel caso in cui lo strumento di lavoro è già connesso alla rete INMP.
Nel caso in cui lo strumento di lavoro non sia connesso alla rete dell'Istituto, si potrà utilizzare un'altra connessione solo garantendo che:

- il dispositivo sia dotato di un antivirus, correttamente configurato ed aggiornato sia come versione del software che come pattern dei virus;
- il sistema operativo del dispositivo e tutti i servizi siano aggiornati dal punto di vista della sicurezza;
- in caso di utilizzo di una rete wi-fi esterna, questa sia adeguatamente protetta.

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

Inoltre, non avvalendosi degli strumenti di navigazione protetta garantita dall'Istituto, sarà cura dell'utente stesso non visitare siti o memorizzare documenti che abbiano un contenuto contrario a norme di legge, all'ordine pubblico e al buon costume. Di seguito è riportato un elenco, non esaustivo, delle categorie di contenuti on-line vietati:

- pornografia;
- anonimizzatori;
- strumenti di manomissione e compromissione dei sistemi;
- vendita di sostanze stupefacenti o altri prodotti illegali.

Relativamente alle connessioni wi-fi fornita dall'Istituto, è vietata l'attestazione sulla rete dell'Istituto di dispositivi non autorizzati che consentano l'accesso in modalità wireless. L'autorizzazione è fornita dalla UOS Sistema Informativo e Statistico.

1.12. Posta elettronica

L'Istituto mette a disposizione del lavoratore un indirizzo di posta elettronica a scopo lavorativo. L'utilizzo della posta elettronica dell'Istituto deve rispettare le disposizioni di legge in materia, l'etica aziendale, gli obblighi di riservatezza e gli standard previsti da specifiche normative interne.
All'utente del servizio di posta elettronica è richiesto di attenersi alle seguenti indicazioni:

- utilizzare esclusivamente il client di posta elettronica standard messo a disposizione dall'Istituto o accedere via web con le modalità di accesso previste dall'Istituto;
- segnalare la ricezione di messaggi con contenuto pericoloso alla UOS Sistema Informativo e Statistico;
- inserire i dati personali, particolari o riservati in un apposito allegato protetto da password o cifratura e mai devono essere contenuti nel corpo del testo del messaggio;
- usare gli strumenti di cifratura dati o firma digitale approvati dalla UOS Sistema Informativo e Statistico per inviare file allegati contenenti informazioni particolari o riservate;
- verificare che la dimensione di un singolo messaggio, inclusi i file allegati, che si vuole inoltrare, non sia superiore al valore di soglia stabilito dalla UOS Sistema Informativo e Statistico, 17 MB;
- usare strumenti di compressione dati per inviare file allegati di dimensioni superiori al limite massimo fissato;
- eliminare dalla cartella <posta in uscita> del proprio client di posta i messaggi superiori al valore limite, al fine di evitare tentativi ripetuti di inoltro automatico;
- adottare politiche di contenimento dell'occupazione dello spazio mailbox assegnato: cancellare o scaricare sul proprio client o su altro supporto autorizzato, periodicamente o in caso di necessità, i messaggi presenti sul mail server.

All'utente dei servizi di posta elettronica non è consentito:

- modificare il proprio client di posta elettronica standard messo a disposizione dall'Istituto;
- utilizzare la casella di un altro utente o condividere la casella personale con altri dipendenti o collaboratori esterni;
- inviare al proprio account di posta personale dati di titolarità INMP, acquisiti in occasioni di lavoro;
- inviare o archiviare sul server di posta elettronica o sulla propria postazione di lavoro messaggi e allegati in violazione di norme di legge. A titolo esemplificativo e non esaustivo non sono consentiti:
    - le richieste, le petizioni e in generale il mailing di massa di qualunque contenuto;
    - gli invii di software, file musicali, video e in generale di qualsiasi tipologia di materiale protetto dalle norme sul diritto d'autore, non prodotti da INMP, o per conto di INMP;

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

- i messaggi e gli allegati dal contenuto contrario a norme di legge, all'ordine pubblico o al buon costume;

- l'uso improprio del servizio, mediante adozione di strumenti atti a mascherare la propria identità;
- inviare o archiviare sul server di posta elettronica o sulla propria postazione di lavoro, messaggi e allegati contenenti informazioni dell'Istituto riservate, con particolare riferimento a:
  - password e altri codici di accesso ai sistemi informatici dell'Istituto;
  - documenti dell'Istituto non crittografati o protetti da password;
- inviare messaggi destinati direttamente o per conoscenza a un elevato numero di utenti, se non indispensabile;
- esprimersi in nome e per conto dell'Istituto senza la preventiva autorizzazione;
- inviare comunicazioni anonime o mascherare la propria identità tramite pseudonimi;
- diffondere notizie a carattere riservato, né inviare documenti di lavoro ad indirizzi di posta elettronica esterni alla rete informatica dell'Istituto, se non protetti da password o crittografati;
- non usare mai la funzionalità dello strumento di posta "rispondi a tutti" e verificare sempre uno a uno i reali interessati alla risposta.

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

2. GESTIONE DEGLI INCIDENTI

Ogni incidente (malfunzionamento PC, indisponibilità dei servizi applicativi o di rete) deve essere segnalato dall'utente, in modo tempestivo, alla UOS Sistema Informativo e Statistico che avvierà il processo di classificazione e risoluzione dell'incidente medesimo. Per gli incidenti che possono determinare una violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, la comunicazione deve essere fatta tempestivamente alla UOS Sistema Informativo e Statistico e al proprio responsabile.

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009

3. DISPOSIZIONI FINALI

Nell'utilizzare gli strumenti informatici messi a disposizione dall'Istituto, il dipendente è tenuto ad usare la diligenza richiesta dalla natura della prestazione dovuta e dall'interesse dell'Istituto, utilizzandoli esclusivamente per ragioni di servizio. Comportamenti difformi da quanto previsto nelle presenti linee guida possono causare gravi rischi alla sicurezza ed all'integrità dei sistemi dell'Istituto.
I comportamenti difformi da quanto previsto nelle presenti linee guida saranno oggetto di sanzione disciplinare nel caso costituiscano violazione del Codice di Comportamento adottato dall'Istituto, nonché di sanzione penale nel caso costituiscano fattispecie di reato.

Istituto Nazionale per la promozione della salute delle popolazioni Migranti e per il contrasto delle malattie della Povertà (INMP)
National Institute for Health, Migration and Poverty (NIHMP)

Via di S. Gallicano 25/a 00153 Roma
Tel. +39 06/58558201 Fax 06/58558401 - info@inmp.it - www.inmp.it
Codice Fiscale e Partita IVA 09694011009