*Ministero dell'istruzione*

*Dipartimento per le risorse umane, finanziarie e strumentali*

*Direzione Generale per i sistemi informativi e la statistica*

# POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

# PER GLI UTENTI DEL SISTEMA INFORMATIVO DELL'ISTRUZIONE

# PER IL PERSONALE ESTERNO AL MINISTERO DELL'ISTRUZIONE

**SOMMARIO**

Fare clic o toccare qui per immettere il testo.

# 1 Riferimenti generali

## 1.1 Traccia delle versioni

| numero versione | data ultima modifica |
|---|---|
| **v. 2.0** | 20/12/2021 |

## 1.2 Scopo della politica

Questo documento fornisce al personale utente del *Sistema Informativo del Ministero dell'Istruzione* una panoramica sulle responsabilità loro spettanti in merito alla gestione ed allo sviluppo della sicurezza delle informazioni, allo scopo di accrescere la cultura della sicurezza e le politiche di utilizzo dei sistemi informativi che il personale utilizza per connettersi alle infrastrutture del Ministero dell'Istruzione. Tramite le presenti politiche il Ministero dell'Istruzione intende agevolare e diffondere la conoscenza delle singole attività che il lettore è responsabilizzato a seguire per garantire l'innalzamento del livello di sicurezza della struttura.

Il termine "sicurezza" si riferisce a tre aspetti distinti:

- **Riservatezza**: Prevenzione contro l'accesso non autorizzato alle informazioni e conformità dell'utilizzo alle linee guida del Garante per il trattamento dei dati personali;
- **Integrità**: Le informazioni non devono risultare alterabili da incidenti o abusi;
- **Disponibilità**: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche opportuni meccanismi organizzativi; misure esclusivamente di natura tecnica, per quanto sofisticate, potrebbero non risultare efficienti laddove usate impropriamente.

### 1.3 Destinatari

La presente politica si applica a tutto il personale non direttamente dipendente del Ministero dell'Istruzione, che si trovi, per necessità di collaborazioni lavorative, ad interagire per via telematica con il personale dell'Amministrazione e/o ad utilizzare strumenti e sistemi informativi forniti dal MI.

## 2 Guida alla lettura del documento

Questo documento contiene le politiche per la sicurezza delle informazioni del Sistema Informativo dell'Istruzione. È possibile leggere la politica per intero o utilizzare il sommario all'inizio del documento per accedere ai singoli capitoli e/o sezioni interessate.

Nel cap. 1 viene definito lo scopo generale della politica e gli utenti destinatari della presente politica.

Nel cap. 3 vengono illustrate le regole di utilizzo del servizio internet, con riguardo ad azioni consentite, non consentite o sconsigliate.

Il cap. 4 stabilisce le regole per l'utilizzo e la gestione della postazione di lavoro, sia fissa che mobile.

Il cap. 5 informa gli utenti sulle modalità di accesso ai servizi dell'amministrazione.

## 3 Regole per l'utilizzo del servizio Internet

Con il presente paragrafo si intende disciplinare l'utilizzo della connessione Internet da parte degli utenti del sistema informativo dell'Istruzione. In particolare, si fa riferimento, a titolo esemplificativo e non esaustivo, ai seguenti principali servizi resi all'utente:

- World Wide Web
- File Transfer Protocol
- Chat
- Forum
- Blog

- Voice over IP
- Podcast.

Nella definizione delle regole d'uso del servizio e delle modalità di controllo, il MI ritiene di grande importanza salvaguardare la libertà di espressione e di pensiero e garantire la tutela dei dati personali degli utenti e dei soggetti terzi. L'Amministrazione, anche sulla base delle direttive del Governo tese a promuovere l'uso delle nuove tecnologie informatiche, considera Internet una risorsa di grande utilità nell'esecuzione delle attività lavorative del personale del MI.

## 3.1 Ambito di applicazione

La presente Politica si applica a:

- tutti i sistemi e le postazioni di lavoro che hanno accesso ad Internet;
- agli amministratori di tale servizio;
- tutti gli utenti dotati di una connessione Internet, nell'ambito del sistema informativo;
- tutte le connessioni ad Internet e le registrazioni a queste connesse (indirizzo mittente, indirizzo destinatario ecc.) effettuate da dipendenti del MI o da altri utenti, amministratori o gestori del servizio.

## 3.2 Requisiti Generali

Il MI considera il servizio Internet come uno strumento di valore e di supporto all'attività lavorativa, che rende possibile l'accesso ad un vasto patrimonio di risorse informative e di strumenti. Il servizio di connessione ad Internet, erogato tramite dei fornitori dei servizi in outsourcing, è proprietà del MI.

**Restrizioni all'uso del servizio**: Gli utenti del servizio Internet sono tenuti ad usarlo responsabilmente, cioè, rispettando le leggi, la presente e altre politiche e procedure del MI e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi Internet può essere totalmente o parzialmente limitato dall'Amministrazione, anche senza preavviso e senza necessità di assenso da parte dell'utente, quando richiesto dalla legge e in conformità ad essa, o in caso di

comprovati motivi che facciano ritenere la violazione della presente politica o delle disposizioni di legge vigenti, o in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

**Monitoraggio del servizio**: Per motivi di sicurezza e di prestazione del servizio tutte le connessioni ad Internet da parte degli utenti abilitati subiscono la registrazione di dati di log quali indirizzo IP mittente e destinatario, data e ora della connessione e URL http richiesto; dati funzionali allo scopo di garantire la qualità del servizio e alla ricostruzione di eventuali incidenti di sicurezza.

I sistemi software sono programmati e configurati in modo da conservare i dati personali relativi agli accessi ad Internet per il tempo necessario a soddisfare esigenze tecniche e di sicurezza, nel rispetto dei principi di cui al GDPR.

Il MI non ispeziona sistematicamente queste registrazioni, tuttavia potrà permettere l'ispezione e l'analisi dei file di log nei seguenti casi:

- su richiesta scritta dell'autorità giudiziaria nei casi previsti dalla normativa vigente;
- per gravi e comprovati motivi (come definiti nel paragrafo *Definizioni* in calce alla presente politica) che facciano credere che siano state violate le disposizioni di legge vigenti o le politiche del MI in materia di sicurezza;
- per atti dovuti (definiti nel paragrafo *Definizioni* in calce alla presente politica);
- in situazioni critiche e di emergenza (definite nel paragrafo *Definizioni*).

Nelle fattispecie sopra indicate sarà eventualmente possibile effettuare il monitoraggio in tempo reale della connessione, attraverso l'utilizzo di strumenti in grado di analizzare la natura ed i contenuti del traffico in ingresso o in uscita.

## 3.3 Requisiti Specifici

Gli utenti del servizio Internet sono informati del fatto che:

- La natura stessa del servizio lo rende insicuro, fonte e veicolo di molte delle minacce alla sicurezza dei sistemi informativi oggi esistenti. Gli utenti pertanto devono esercitare la

massima cautela nel suo utilizzo, nell'ambito dei vari servizi disponibili.

- Internet è una rete mondiale di computer che contiene milioni di pagine di informazioni; parte di queste possono avere contenuti offensivi o illegali, con cui si può entrare accidentalmente in contatto, ad esempio attraverso interrogazioni a motori di ricerca effettuate per scopi "innocui". Inoltre, la diffusione del proprio indirizzo di posta elettronica mediante Internet, ad esempio inserendolo in mailing list non adeguatamente gestite, può facilmente portare a essere fatti oggetto di invii di messaggi indesiderati di posta. Per queste ragioni il MI non si ritiene responsabile per il materiale cui gli utenti hanno avuto accesso o che abbiano scaricato, ma cerca di minimizzare i rischi connessi all'uso di Internet mediante l'applicazione della presente Politica, cui gli utenti sono tenuti ad attenersi. A tale scopo il MI si riserva altresì il diritto di bloccare l'accesso a siti Internet aventi contenuto offensivo o illegale mediante uso di appositi strumenti software.
- La tracciatura delle connessioni Internet, effettuata nelle modalità di cui sopra, originanti o destinate ad apparati elettronici forniti dal MI, possono costituire registrazioni di attività svolte dall'Amministrazione (ricezione o invio di informazioni scambiate tra uffici e personale del MI, tra il MI ed enti o società esterne o singoli cittadini). È possibile quindi che venga richiesto l'accesso alle registrazioni per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Amministrazione. Il MI non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge, quali quelli derivanti dalla tutela dei dati personali, ed altre normative applicabili.

L'uso della connessione Internet nell'ambito del servizio informativo dell'Istruzione è soggetto alle seguenti condizioni:

- **Proibizioni**. È fatto divieto a tutti gli utenti di utilizzare il collegamento Internet per inviare o inserire nell'ambito di blog, forum di discussione o servizi similari, messaggi di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio o testo che possa arrecare danno alla reputazione del MI. È vietato

scaricare o trasmettere materiale osceno, diffamatorio, intimidatorio, discriminatorio o comunque contrario alla legge sotto qualunque forma (immagini, testi, filmati, registrazioni vocali ecc.). È vietato trasmettere o scaricare e installare materiale protetto da *copyright*. È inoltre vietato l'uso della connessione Internet a scopi commerciali o di profitto personale e per attività illegali. È proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi che facciano richiesta di questo tipo di informazioni. È infine proibito accedere ad Internet dalle postazioni di lavoro del MI aggirando i sistemi di sicurezza predisposti allo scopo dal MI, utilizzando mezzi di accesso diretto non autorizzati (smartphone, hotspot, etc.).

- **Uso Personale**. È consentito l'utilizzo della connessione Internet, in modo occasionale, a fini privati e personali, purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo non: (i) sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di collegamento dell'Amministrazione; (ii) sia causa di oneri aggiuntivi per l'Amministrazione; o (iii) interferisca con le attività lavorative dell'utente o con altri obblighi dello stesso verso l'Amministrazione.

Va tenuto presente che le risorse di rete e di memoria dei computer sono limitate. Tutti gli utenti hanno pertanto la responsabilità di farne un uso oculato evitando di sprecare deliberatamente dette risorse o di monopolizzarne l'uso a discapito degli altri utenti. Gli utenti devono pertanto astenersi da:

- inviare messaggi di posta elettronica ad un gran numero di destinatari o partecipare a "Catene di S. Antonio";
- spendere eccessiva parte del proprio tempo navigando su Internet, se non per scopi lavorativi;
- partecipare a giochi online o a *chat*;
- caricare o scaricare file di grandi dimensioni;
- accedere a trasmissioni in streaming audio o video, se non per scopi lavorativi;
- generare immotivatamente carico eccessivo sulle strutture elaborative del MI per scopi privati o personali.

L'Amministrazione presuppone quindi che l'utente decida di utilizzare la connessione Internet per

scopi personali avendone preliminarmente e attentamente valutato l'opportunità.

### 3.4 Violazioni

Il personale che contravviene alle norme indicate nel presente documento, stanti le responsabilità individuali di tipo civile e penale verso terze parti offese, potrà essere oggetto di sanzioni di tipo amministrativo la cui entità e modalità di erogazione saranno definite secondo le procedure previste dai contratti di lavoro attualmente vigenti.

## 4 Regole per l'utilizzo e la gestione delle postazioni di lavoro

### 4.1 Finalità

La presente politica disciplina l'utilizzo delle postazioni di lavoro (PdL) in relazione all'infrastruttura tecnologica del Ministero dell'Istruzione, e l'accesso ai sistemi ed ai servizi informatici per gli utenti del sistema informativo.

Nella definizione delle regole d'uso degli strumenti informatici e delle modalità di controllo, il MI ritiene di grande importanza salvaguardare la libertà di espressione e di pensiero e garantire la tutela dei dati personali degli utenti e dei soggetti terzi. La presente Politica rispetta quindi i principi basilari esposti, nel contesto degli obblighi legali e delle politiche di sicurezza dell'Amministrazione.

La presente politica vale anche come informativa sulle finalità e modalità del trattamento dei dati personali degli utenti, ricavabili dalle attività di controllo tecnico svolte sul sistema, ai sensi del Decreto Legislativo n.101/2018, in seguito riferito come GDPR. Per i dettagli in relazione alla informativa sulle finalità e modalità del trattamento dei dati personali si rimanda al § 9.

Scopo della presente politica è assicurare che:

a) Gli utenti del sistema informativo dell'istruzione acquisiscano piena consapevolezza e comprensione delle norme, regole e procedure operative emanate dall'Amministrazione in merito all'utilizzo della loro postazione di lavoro ed accesso ai sistemi ed ai servizi informatici disponibili;

b) La postazione di lavoro sia utilizzata dagli utenti in conformità alle disposizioni di cui alla precedente lettera a);

c) Gli utenti del sistema informativo dell'istruzione siano informati e rispettino le disposizioni di legge e regolamentari vigenti, incluse quelle relative alla tutela dei dati personali e della sicurezza delle informazioni;

d) l'accesso al sistema sia fruibile con la massima continuità ed affidabilità.

## 4.2 Considerazioni di carattere generale

Il MI considera le postazioni di lavoro come uno strumento di valore e di supporto fondamentale all'attività lavorativa, tramite il quale è possibile accedere ad un vasto patrimonio di risorse informative e di strumenti, ivi compreso il sistema informativo dell'istruzione e i servizi informatici resi disponibili nell'ambito del sistema stesso.

Per Postazione di Lavoro (PdL) si intende l'insieme minimo dei dispositivi, messi a disposizione dall'Amministrazione, necessari alla produttività individuale del personale; la postazione di lavoro può essere classificata in:

- Postazione fissa, costituita da client (tastiera, mouse, monitor, unità centrale, lettore e masterizzatore unità ottiche) e stampante;
- Postazione mobile, costituita da notebook, palmari, smartphone e tablet di proprietà del MI.

Le caratteristiche della postazione di lavoro sono determinate dalle applicazioni fruibili dalla postazione di lavoro e sono suscettibili di adeguamenti sulla base dell'evoluzione tecnologica. Il software applicativo installato è quello strettamente necessario a garantire l'espletamento delle funzioni/compiti di lavoro assegnategli.

Gli utenti del sistema informativo dell'istruzione sono tenuti ad utilizzare la postazione di lavoro, i sistemi ed i servizi informatici in modo responsabile ed esclusivamente per scopi legati alle attività svolte per conto dell'Amministrazione, cioè, rispettando le leggi, la presente e altre politiche e procedure del MI e secondo normali standard di correttezza, buona fede e diligenza professionale. L'accesso ai sistemi ed ai servizi informatici e la possibilità di utilizzo delle postazioni di lavoro, può essere totalmente o parzialmente limitato dall'Amministrazione, anche senza preavviso e senza

necessità di assenso da parte dell'utente, quando richiesto dalla legge e in conformità ad essa, o in caso di comprovati motivi che facciano ritenere necessaria la violazione della presente politica o delle disposizioni di legge vigenti, o in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

Per motivi di sicurezza e di prestazioni, l'accesso ai sistemi e ai servizi informatici è consentito solo attraverso procedure di autorizzazione che prevedono le funzioni di identificazione ed autenticazione. Solo attraverso un processo formale di registrazione e de-registrazione l'utente sarà autorizzato ad accedere ai servizi e sistemi per i quali è stato abilitato. Tale processo prevede:

- L'uso di credenziali uniche (in modo tale che gli utenti possano essere collegati alle proprie azioni ed essere resi in tal modo responsabili);
- il controllo che l'utente abbia l'autorizzazione ad accedere al servizio richiesto;
- il controllo che il livello di accesso concesso sia appropriato;
- il mantenimento di una registrazione formale di tutte le persone che possono usare i vari servizi informatici.

I sistemi utilizzati dall'utente possono registrare le informazioni, in appositi file di log, conservati per il tempo necessario ad erogare il servizio e ad adempiere gli obblighi previsti dalla normativa vigente ed imposti dalle autorità competenti.

## 4.3 Regole di utilizzo delle Postazioni di lavoro

Il MI mette a disposizione degli utenti le postazioni di lavoro per svolgere le loro rispettive mansioni. Il personale utente del Sistema Informativo dell'istruzione è informato del fatto che per una corretta fruizione dei servizi e al fine di tutelare la riservatezza, l'integrità e disponibilità delle informazioni gestite tramite il sistema, è necessario che osservi alcune norme comportamentali relative alla gestione degli strumenti informatici messi a disposizione dall'Amministrazione.

In particolare:

1. L'utente di ciascuna PdL è responsabile dell'utilizzo dei sistemi informatici messi a sua disposizione per lo svolgimento delle mansioni affidategli. In tal senso ciascun utente è ritenuto responsabile del corretto utilizzo dei propri strumenti di identificazione personale, della segretezza dei propri codici d'accesso e delle operazioni compiute tramite la propria utenza;
2. In linea generale, ciascun soggetto autorizzato è tenuto ad adottare ogni opportuna cautela atta ad evitare danni, temporanei o permanenti, a sistemi informatici o telematici, nonché a dati, documenti e comunicazioni scritte;
3. prima di allontanarsi dalla postazione, anche momentaneamente, devono essere attivati i sistemi di protezione esistenti per evitare ogni accesso non autorizzato (ad esempio, blocco dello schermo tramite Win+L con password locale).
4. Al termine della sessione di lavoro, ovvero al termine dell'orario lavorativo, la postazione di lavoro deve essere spenta.
5. L'utente è tenuto alla modifica della password di default al trascorrere di 24 dal primo accesso al sistema e a cambiarla regolarmente (l'assegnazione della password di "default" da parte della gestione del sistema informativo avviene in caso di nuovo utente, perdita o blocco della password).

   In caso di prolungata assenza o impedimento dell'utente, al fine di assicurare la disponibilità di dati o strumenti elettronici in situazioni che rendano indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema [GDPR, Decreto Legislativo n.101/2018] il dirigente dell'ufficio potrà richiedere all'Amministratore del sistema di accedere alla postazione di lavoro dell'utente ed ai sistemi e applicazioni per le quali l'utente risulta abilitato.
6. La password deve essere custodita in maniera diligente e cambiata regolarmente, seguendo nella scelta alcune "regole di buona condotta":
   a) non trascrivere la password su fogli, agendine, post-it facilmente accessibili a terzi;
   b) non scegliere password corrispondenti a parole che possano essere presenti in un dizionario;

c) scegliere una password che non sia stata precedentemente utilizzata in ambito personale o lavorativo, per non esporre a pericolo i dati del MI in caso di Data Breach su piattaforme esterne non afferenti ad attività lavorativa;
d) non scegliere una password facilmente associabile ad informazioni relative all'utente, quali ad esempio il nome proprio, il nome di familiari, il codice fiscale, i numeri di telefono, la data di nascita, la user-id, ecc.;
e) non utilizzare sequenze digitate alla tastiera (ad esempio: qwerty);
f) evitare di modificare la password facendo solo delle piccole modifiche come numerazioni progressive, ecc
g) Nel caso in cui una password perda di segretezza (accidentale smarrimento della stessa, divulgazione a terzi per motivi di lavoro, ecc.), l'utente si deve attivare per la sua immediata sostituzione.

7. L'utilizzo di periferiche (penne USB, dischi esterni, etc…) è soggetto ad una preventiva scansione da parte del software antivirus fornito sul sistema dal supporto IT, aggiornato regolarmente.
8. Qualora l'utente ravvisi eventuali anomalie nell'utilizzo delle risorse informatiche a sua disposizione, è tenuto a dare notifica al Referente Informatico, il quale, in collaborazione con le funzioni di sicurezza del MI, attiva le procedure di Incident Management.
9. Tutto il personale è chiamato ad osservare una politica della "scrivania pulita" e dello "schermo pulito" relativamente ai documenti cartacei e ai mezzi di immagazzinamento rimuovibili e all'uso degli impianti di elaborazione delle informazioni, allo scopo di ridurre i rischi di accessi non autorizzati, perdita di informazioni, danni alle informazioni, durante o al di fuori delle normali ore di lavoro. Documenti cartacei, supporti magnetici/ottici e notebook, quando non usati, devono essere riposti sottochiave in armadietti, specie al di fuori delle ore di lavoro o quando gli uffici rimangono incustoditi.

10. L'utente è tenuto ad effettuare il backup con frequenza almeno settimanale tramite le applicazioni fornite dall'Amministrazione, con particolare riguardo alla posta elettronica e ai documenti di ambito lavorativo, oltre a cifrare le informazioni sensibili contenute nella postazione di lavoro tramite i software forniti dal MI. Il backup può essere effettuato facendo una copia della cartella presente nel percorso D:\Users\MIxxxxx, relativa al proprio nome utente.
11. Tutela legale del software: in relazione alle attività di installazione / duplicazione del software, tenuto conto del disposto della Legge 22.4.1941 n. 633 ("Protezione del diritto d'autore e di altri diritti connessi al suo esercizio"), del D.Lgs. 29.12.1992 n. 518 ("Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaborazione") l'Amministrazione conferma l'obbligo dell'osservanza dei seguenti principi:
    - tutti i computer sono forniti con istanze autorizzate dei programmi;
    - qualsiasi duplicazione non autorizzata di software concesso in licenza, esclusa quella per scopi di backup e archiviazione, costituisce violazione delle norme a tutela del diritto d'autore.

### 4.3.1 Postazioni di lavoro mobili

Quando si usano notebook, palmari e computer portatili di proprietà del MI, si deve prestare particolare attenzione a far sì che le eventuali informazioni appartenenti al Sistema Informativo dell'Istruzione non risultino compromesse al momento della rimozione dell'apparato dalle zone protette. **Oltre a quanto previsto nei puti precedenti**, le politiche di utilizzo delle postazioni di lavoro mobili, o più generalmente di apparecchiature mobili, prevedono:

1. Il dispositivo deve essere utilizzato esclusivamente dalla persona autorizzata e solo ai fini strettamente connessi alle attività dell'Amministrazione.

2. L'utente deve evitare di lasciare incustodito qualsiasi dispositivo mobile, assicurandolo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio forniti dall'Amministrazione e prestando particolare attenzione soprattutto ai momenti in cui la postazione di lavoro non si trova all'interno del luogo di lavoro, ad esempio durante il trasporto in auto. In caso di viaggio, la postazione di lavoro deve essere tassativamente trasportata come bagaglio a mano.
3. In caso di smarrimento o furto del dispositivo mobile, oltre a sporgere regolare denuncia all'autorità competente, è necessario informare tempestivamente il proprio Referente Informatico, che è incaricato di attivare immediatamente la procedura di Data Breach e di informare tempestivamente il dirigente dell'ufficio competente, comunicando i dati personali e sensibili contenuti all'interno del dispositivo.
4. L'utente deve utilizzare protezioni fisiche (armadietti o cassetti chiusi a chiave, cavi antifurto) quando gli apparecchi non sono in uso.
5. L'utente deve osservare le istruzioni del fabbricante per la protezione durante il trasporto nei confronti di urti, campi elettromagnetici, sbalzi di temperatura, ecc.
6. Come protezione logica è prevista l'installazione di software antivirus, di cui l'utente non deve in alcun caso impedire il costante aggiornamento e non deve assolutamente disabilitare. Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un malware oppure si sospetti la presenza di un virus non rilevato dal programma antivirus, è necessario segnalarlo all'assistenza tecnica. Si raccomanda di non scaricare e né tantomeno aprire file sospetti provenienti via e-mail da mittenti sconosciuti. Tali file possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in esso contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

7. L'utilizzo di periferiche (penne USB, dischi esterni, ecc.) è vivamente sconsigliato, tuttavia ogni periferica che venga inserita nella postazione di lavoro è soggetta ad una preventiva scansione da parte del suddetto software antivirus. I supporti rimovibili che contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri soggetti non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati opportunamente formattati al fine di non consentire il recupero dei dati rimossi. Il trasferimento di file contenenti dati personali su supporti rimovibili è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. Si raccomanda di proteggere con password i supporti rimovibili contenenti dati personali.

L'uso della postazione di lavoro nell'ambito del sistema informativo dell'Istruzione è soggetto alle seguenti condizioni:

- **Proibizioni**. È vietato l'uso della postazione di lavoro per scopi commerciali o di profitto personale e per attività illegali. Ricordando che la responsabilità delle operazioni compiute tramite una utenza è sempre del legittimo titolare della stessa, anche se compiute in sua assenza, la password (o corrispondente garanzia di identità, sia SPID, OTP, o biometrica) non deve essere comunicata a nessuno, neppure ai gestori del Sistema Informativo o ai propri Responsabili. È vietato installare sulla postazione di lavoro e utilizzare strumenti che potenzialmente sono in grado di consentire l'accesso non autorizzato alle risorse informatiche (ad es. cracker, programmi di condivisione quali IRC, …). È altresì vietato installare sui PC software non autorizzati o usare versioni portable di software o hardware (hotspot dallo smartphone) che permettano l'accesso in desktop remoto, scansioni e attività in rete diverse dall'accesso alla rete internet e alle directory condivise, bypassando le misure di sicurezza esistenti.

In aggiunta a ciò, tutto quanto non è esplicitamente permesso è vietato.

# 5 Accesso ai servizi

Per accedere ai servizi e alle dotazioni del MI, è sempre necessario un account istituzionale, dotato di nome utente e password. Per evitare la diffusione di dati sensibili volontaria e involontaria, il Ministero dell'Istruzione potrebbe richiedere, in alcuni casi, l'autenticazione a più fattori. Questa pratica aumenta il livello di sicurezza e riservatezza delle informazioni e permette l'accesso solamente al personale del MI, che abbia opportunamente verificato la propria identità; in questo modo, in caso di furto o di smarrimento delle password o delle dotazioni istituzionali ovvero in caso di tentativi di accesso non autorizzati da parte di terzi, le informazioni contenute nei dispositivi e nei servizi offerti dall'Amministrazione godono di un ulteriore strato di protezione.

Per rendere fruibile il servizio di autenticazione a più fattori potrebbe essere richiesto al dipendente di fornire al MI un numero di telefono cui inviare un sms di verifica oppure potrebbe essere richiesta l'installazione di un'apposita applicazione sullo smartphone del personale. In altri casi, invece, l'Amministrazione potrebbe fornire al dipendente un dispositivo che generi un codice OTP di durata temporanea per consentire l'accesso.

Il personale dipendente del Ministero dell'Istruzione ha l'onere di custodire e proteggere al meglio delle proprie possibilità, i sistemi di autenticazione che vengono forniti dall'Amministrazione, ivi comprese credenziali di accesso e le dotazioni su cui vengono configurate le autenticazioni a fattore multiplo. In caso di smarrimento o furto dei dispositivi sopra citati, il personale del MI è tenuto ad informare tempestivamente il proprio Referente Informatico, che provvede a richiedere il blocco o la modifica di tali modalità di accesso.

# 6 Definizioni

**Asset:** Informazione o risorsa di valore che è necessario salvaguardare.

**Attacco alla Sicurezza:** Qualsiasi azione volta a compromettere la Sicurezza dell'informazione posseduta da un'organizzazione.

**Atti dovuti:** circostanze in base alle quali la mancanza di adeguate azioni può comportare danni

significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte.

**Availability (Disponibilità):** Assicurazione che gli utenti autorizzati possano accedere alle informazioni ed alle risorse informatiche quando richiesto.

**Browser:** programma informatico atto alla navigazione in internet.

**Cloud:** L'archiviazione, l'elaborazione o la trasmissione dati cui si accede tramite internet protetti da un fornitore esterno.

**Confidentiality (Confidenzialità, Riservatezza):** Assicurazione che l'informazione è accessibile solo agli utenti autorizzati ad accedervi.

**Crack:** è un'applicazione che aggira le protezioni di un programma in modo da permetterne l'uso anche non avendolo acquistato.

**Data Breach**: violazione dei dati personali, rilascio intenzionale o non intenzionale di informazioni sicure o private / riservate in un ambiente non attendibile.

**DGSI:** Direzione Generale Sistemi Informativi MI.

**End-of-life / End-of-support:** un termine usato rispetto a un prodotto fornito ai clienti, indicando che il prodotto è alla fine della sua vita utile e che un fornitore interrompe la commercializzazione, la vendita o la rilavorazione per sostenerlo.

**Grave e comprovato motivo:** evidenza oggettiva, non basata quindi su semplici sospetti o illazioni, che dimostra l'avvenuta violazione di disposizioni di leggi vigenti o delle politiche di sicurezza dell'Amministrazione.

**Information Security (Sicurezza delle Informazioni – SI):** Salvaguardia delle caratteristiche di availability, confidentiality e integrity dell'informazione.

**Integrity (Integrità):** Salvaguardia dell'accuratezza e della completezza dell'informazione e dei beni collegati.

**ISMS (Information Security Management System) e SGSI (Sistema di Gestione per la Sicurezza delle**

**Informazioni):** Parte del sistema complessivo di gestione, basato su un approccio di business risk, con lo scopo di stabilire, attuare, monitorare, riesaminare, mantenere e migliorare l'information security.

**Malware:** Programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico.

**Minaccia:** Una potenziale causa di danni alle risorse aziendali.

**MI:** Ministero dell'Istruzione.

**Ministero o Amministrazione:** si intende il Ministero dell'Istruzione.

**Open-source:** Software non protetto da copyright e liberamente modificabile dagli utenti.

**Password Reuse**: La partica di utilizzare password già in uso presso altri account o molto simili tra loro.

**Politica:** In ISO 9001 e ISO 27001 è la politica, come linea di indirizzo strategico definita dal vertice dell'organizzazione.

**Pop-up:** Finestre o riquadri, che compaiono automaticamente durante l'uso di un'applicazione ed in determinate situazioni, per attirare l'attenzione dell'utente.

**Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

**Rischio per la Sicurezza**: La possibilità che una certa minaccia sfrutti le vulnerabilità delle risorse aziendali per arrecare danno alle risorse stesse.

**Rischio residuo:** Il rischio per la Sicurezza che rimane in seguito all'attuazione di tecniche di Sicurezza.

**Risk Acceptance (Accettazione del rischio):** Decisione di accettare un rischio.

**Risk Analysis (Analisi del rischio):** Uso sistematico di informazioni per identificare le sorgenti del rischio e per stimare il rischio.

**Risk Assessment:** Processo complessivo di Risk Analysis e Risk Evaluation: è il processo di identificazione dei rischi per la sicurezza e di individuazione delle loro magnitudo

**Risk Evaluation (Valutazione del rischio):** Processo di comparazione tra il rischio stimato ed i criteri di

rischio stabiliti per determinare la significatività del rischio.

**Risk Management (Gestione del rischio):** Attività coordinate per dirigere e controllare l'organizzazione in relazione al rischio: è il processo di identificazione e di applicazione di tecniche di Sicurezza all'interno di un'organizzazione (ai sistemi, alle applicazioni ed ai servizi), proporzionali ai rischi Identificati.

**Risk Treatment (Trattamento del rischio):** Processo per trattare la selezione e l'attuazione delle misure atte a modificare il rischio.

**Risorsa aziendale:** Tutto ciò che ha un valore per l'azienda: sistemi, applicazioni e servizi

**Servizio di Sicurezza:** Servizio che garantisce la Sicurezza dei sistemi di elaborazione e di trasmissione dati di un'organizzazione. I servizi di Sicurezza, allo scopo di contenere gli attacchi, utilizzano una o più tecniche di Sicurezza.

**Situazioni critiche o di emergenza:** circostanze in cui la tempestività d'azione è di fondamentale importanza al fine di evitare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte o l'interruzione dei servizi informatici e la continuità operativa dei processi dell'Amministrazione.

**Software:** programma informatico.

**Tecnica di Sicurezza:** Una procedura, una regola o un meccanismo in grado di ridurre i rischi di Sicurezza.

**Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

**USP:** Uffici Scolastici Provinciali.

**USR:** Uffici Scolastici Regionali (Direzioni Regionali e USP).

**Utente**: persona fisica abilitata all'utilizzo del servizio di posta elettronica.

**VPN**: Virtual Private Network (Rete privata virtuale)

**Vulnerabilità:** Una debolezza in una risorsa o in un gruppo di risorse che può essere sfruttata per arrecare danni alle risorse.

# 7 Riferimenti normativi

- Regolamento Europeo 27 aprile 2016, n. 679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- Decreto Legislativo n. 101/2018 – Adeguamento al Regolamento UE 2016/679
- Decreto Legislativo n. 82/2005 – Codice dell'amministrazione digitale
- Decreto Legislativo n. 196/2003 e s.m.i. – Codice in materia di protezione dei dati personali.
- Provvedimento del Garante per la protezione dei dati personali n. 157 del 30 luglio
- Legge 124/2015 in materia di riorganizzazione delle amministrazioni pubbliche.
- Legge 248/2000 in materia di tutela del diritto d'autore.