



## *Ministero della Pubblica Istruzione*

# **POLITICHE DI UTILIZZO DELLE POSTAZIONI DI LAVORO ED ACCESSO AI SISTEMI ED AI SERVIZI INFORMATICI PER GLI UTENTI DEL SISTEMA INFORMATIVO DELL'ISTRUZIONE**

## **1 PREMESSA**

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

Nella definizione delle regole d'uso degli strumenti informatici e delle modalità di controllo, il MPI ritiene di grande importanza salvaguardare la libertà di espressione e di pensiero e la garanzia della privacy dell'individuo. Questa Politica rispetta quindi i principi basilari esposti, nel contesto delle obbligazioni legali e delle politiche di sicurezza dell'Amministrazione.

La presente politica vale anche come informativa sulle finalità e modalità del trattamento dei dati personali, ricavabili dalle attività di controllo tecnico svolte sul sistema, ai sensi dell'art. 13 della legge 196/2003.

## **2 SCOPO**

Scopo della presente politica è assicurare che:

- a) gli utenti del sistema informativo dell'istruzione siano informati circa le norme, regole, e procedure operative emanate dall'Amministrazione in merito all'utilizzo della postazione di lavoro ed accesso ai sistemi ed ai servizi informatici disponibili.
- b) la postazione di lavoro sia utilizzato dagli utenti in conformità a tali disposizioni;
- c) gli utenti del sistema informativo dell'istruzione siano informati in merito ai concetti di privacy e di sicurezza delle informazioni applicabili all'utilizzo delle postazioni di lavoro e del sistema informativo;
- d) l'accesso al sistema sia fruibile con la massima continuità ed affidabilità.

## **3 AMPIEZZA**

La presente Politica si applica a:

- tutti i sistemi e le postazioni di lavoro;
- agli amministratori di tale servizio;

- tutti gli utenti dotati di una connessione al sistema informativo dell'istruzione, appartenenti alle seguenti categorie di personale:
  - personale amministrativo del MPI;
  - docenti comandati;
  - personale esterno all'amministrazione (monitore, consulenti, ecc.);
  - personale amministrativo delle scuole<sup>1</sup>
- tutte le connessioni al sistema informativo dell'istruzione e le registrazioni a queste connesse effettuate da dipendenti del MPI o da altri utenti, amministratori o gestori del servizio.

## 4 REQUISITI GENERALI

- a) **Finalità del servizio.** Il MPI 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.
- b) **Restrizioni all'uso del servizio.** Gli utenti del sistema informativo dell'istruzione sono tenuti ad utilizzare la postazione di lavoro, i sistemi ed i servizi informatici in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche e procedure del MPI 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 la violazione della presente politica o delle disposizioni di legge vigenti, o in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili. Per maggiori informazioni circa le condizioni d'uso e la configurazione delle Postazioni di lavoro si rimanda alla lettura del documento di Configurazione delle politiche di sicurezza per le PdL (ID doc. *AD-SI-POL-Configurazione di sicurezza delle PdL-1.1.doc*) pubblicato sul sito Intranet nella sezione ***Sicurezza delle Informazioni***.

---

<sup>1</sup> In questo caso le regole fissate dalla politica sono vincolanti per quanto riguarda l'accesso ai sistemi e ai servizi informatici del MPI, mentre sono consigliabili per quanto riguarda la gestione delle postazioni di lavoro della scuola che rimane di esclusiva responsabilità della stessa;

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

- ❑ L'uso di *user ID* 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;
- ❑ di mantenere una registrazione formale di tutte le persone che possono usare i vari servizi informatici; la registrazione riguarda almeno i seguenti dati della persona:
  - Nome e cognome
  - Motivazione all'accesso
  - Data di concessione/revoca dell'autorizzazione
  - Livello di autorizzazione concesso
  - Identificativo o userid assegnato;

I sistemi utilizzati dall'utente registrano, in appositi file di log, conservati per un periodo di due anni, le seguenti informazioni:

Tipologia dati	Contenuto
Log di sistema	user-id, orario login e logout
	user-id, accesso a specifiche risorse (file, ecc)
	DHCP: MAC address – indirizzo IP utente (collegamento tra indirizzo e stazione di lavoro utente)
Log applicativi	operazioni effettuate da un singolo utente su dati di esercizio

Tab. 1 Contenuto file di log

## 5 REQUISITI SPECIFICI

### 5.1 AVVERTENZE

Gli utenti del Sistema Informativo dell'istruzione sono avvisati 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 l'utente osservi alcune norme comportamentali relative alla gestione degli strumenti informatici messi a sua disposizione.

In particolare:

1. In via generale il singolo 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. Prima di allontanarsi, anche momentaneamente, devono essere attivati i sistemi di protezione esistenti relativamente alla Postazione di Lavoro (ad esempio, blocco

tramite Ctrl-Alt-Canc con password locale). La Postazione di Lavoro non può essere lasciata incustodita, anche per brevi periodi, con la sessione attiva;

3. L'assegnazione della password di "default" da parte dell'Addetto alla gestione del sistema informativo avviene in caso di nuovo utente, perdita o blocco della password, l'utente è tenuto alla modifica della password al primo accesso e a cambiarla in ogni momento, seguendo le istruzioni contenute nel par. 2.1.2 e nel par. 2.5.4 del documento "Il DESKTOP Guida di riferimento" (nome file *GUIDAUTENTEDESKTOP-01A.pdf*) presente sulla propria Postazione di Lavoro. La nuova password sarà "propagata" su tutti i server dove è stata definita la user-id dell'utente.
4. Al fine di assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'utente, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema" [Regola numero 10 del disciplinare tecnico allegato B della 196/03], il responsabile della sicurezza dell'ufficio potrà richiedere all'Amministratore del sistema, di accedere, *medio tempore*, alla postazione di lavoro dell'utente ed ai sistemi e applicazioni per le quali l'utente risulta abilitato, utilizzando l'apposito modulo di richiesta della Carta Servizi (CS-H-MOD-PASSWORDUTENTI\_INFRASTRUTTURA) riportato nell'allegato 1 della presente politica. Questa modalità non è applicabile al personale amministrativo delle scuole.
5. La password deve essere custodita in maniera diligente e cambiata tempestivamente qualora l'utente ravvisi eventuali anomalie nell'utilizzo delle risorse informatiche, delle quali è tenuto a dare notifica al suo Responsabile o alla funzione sicurezza del MPI.
6. È necessario seguire alcune "regole di buona condotta" nella scelta delle password:
  - a) Non scegliere parole che possono essere presenti in un dizionario
  - b) 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 user-id, ecc.
  - c) Non utilizzare sequenze digitate alla tastiera (ad esempio: qwerty)
7. Tutto il personale è chiamato ad osservare una politica della "scrivania pulita" e dello "schermo pulito" relativamente alle carte 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. Di seguito si riportano le principali caratteristiche della politica:

- ❑ Carte, supporti magnetici/ottici e notebook, quando non usati, devono essere riposti sotto chiave in armadietti, specie al di fuori delle ore di lavoro o quando gli uffici rimangono incustoditi;
8. Quando si usano notebook, palmari e computer portatili si deve prestare particolare attenzione a far sì che le eventuali informazioni appartenenti al Sistema Informativo dell'Istruzione non risultino compromesse. Di seguito si riportano le principali regole generali definite per l'utilizzo delle apparecchiature portatili: Le linee guida per l'utente sono:
- ❑ Evitare di lasciare incustoditi i PC portatili
  - ❑ Osservare le istruzioni del fabbricante per la protezione durante il trasporto nei confronti di urti, campi elettromagnetici, sbalzi di temperatura, ecc;
  - ❑ Come protezione logica è prevista l'installazione di software antivirus, che l'utente non deve disabilitare e provvedere al suo costante aggiornamento.
  - ❑ Effettuare un backup almeno settimanale;
9. Tutela legale del software: in relazione alle attività di installazione / duplicazione del software, tenuto conto del disposto della Legge 22.4.1941 n. 633 (Diritto d'autore), del D.L. 29.12.1992 n. 518 (Tutela giuridica dei programmi per elaborazione) l'Amministrazione conferma l'obbligo dell'osservanza dei seguenti principi:
- ❑ Qualsiasi duplicazione di software concesso in licenza, esclusa quella per scopi di backup e archiviazione, costituisce violazione delle norme a tutela del diritto d'autore;
  - ❑ Qualsiasi programma software concesso in licenza è da usarsi su di un unico computer alla volta;
  - ❑ Tutti i computer sono forniti con copie autorizzate dei programmi installati;
  - ❑ L'Amministrazione non assume responsabilità in merito all'installazione e/o duplicazione non autorizzata di materiale soggetto a proprietà intellettuale di terzi da parte dei propri dipendenti;
  - ❑ I dipendenti che effettueranno tale operazione per scopi diversi dal backup o installeranno o comunque utilizzeranno copie non autorizzate di materiale soggetto a proprietà intellettuale di terzi sono soggetti a sanzioni da parte delle Società licenziatrici stesse.

## 5.2 **USO CONSENTITO**

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

1. **Proibizioni.** E' vietato installare materiale protetto da copyright. E' inoltre vietato l'uso della postazione di lavoro nell'ambito del servizio informativo dell'Istruzione a 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 non deve essere comunicata a nessuno, neppure ai gestori del Sistema Informativo o ai propri Responsabili. Essa deve essere memorizzata dall'utente che non deve trascriverla in nessun luogo.
2. **Uso Personale.** E' consentito l'utilizzo della postazione di lavoro, in modo saltuario, 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. Al riguardo va tenuto ben 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.

L'Amministrazione presuppone quindi che l'utente decida di utilizzare la postazione di lavoro per scopi personali avendone preliminarmente e attentamente valutato l'opportunità.

Tutto quanto non esplicitamente permesso è vietato.

## 5.3 **SICUREZZA E RISERVATEZZA**

1. Oltre a quanto indicato al par. 5.1, gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione può avere, saltuariamente e per esigenze di servizio la necessità di:
  - analizzare i dati risultanti dai file di log delle connessioni al sistema informativo dell'istruzione.
  - Utilizzare la funzione di controllo remoto delle postazioni di lavoroTale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora di verificassero i casi citati.
2. Il MPI si pone come obiettivo fondamentale la disponibilità, riservatezza ed integrità delle informazioni e dei sistemi di gestione del **patrimonio** informativo dell'Amministrazione. Va comunque ricordato che la sicurezza non è un problema affrontabile solo dal punto di vista tecnologico ed quindi indispensabile che l'utente stesso provveda ad attuare le azioni adeguate a proteggere le informazioni ed i sistemi dalle varie minacce, usando tutti i mezzi disponibili, e tenendo una condotta responsabile e professionale

## **6 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.

## 7 ALLEGATO 1 – Carta Servizi .

Il gestore e la DGSI hanno predisposto un processo per soddisfare le seguenti richieste:

- Abilitazione/Disabilitazione Applicazioni (pe. Protocollo, RAP, Organizzazione e Sicurezza, Dataware house)
- Abilitazione/Disabilitazione Cambio Polo
- Abilitazione/Disabilitazione servizi laptop (pe.RAS, VPN)
- Abilitazione/Disabilitazione uso liste di distribuzione
- Abilitazione/Disabilitazione Utenza Internet
- Restore di dati da cartella pubblica
- Creazione/Cancellazione utenze Posta Elettronica
- Distribuzione software
- Emissione badge di accesso al SIMPI.
- Gestione Password (reset e modifica)
- Gestione Utenze di Dominio (creazione, modifica e cancellazione)
- Migrazione utenze Posta Elettronica
- PdL Aggiuntiva
- Riconfigurazione Software PdL
- Spostamento PdL.

Il processo è stato denominato IMAC (Installazione, spostamento, aggiunta o cambiamento) e si basa su un modulo di richiesta chiamato Carta Servizi, in cui sono indicate le informazioni necessarie alla gestione della richiesta.

L'attivazione del processo avviene attraverso l'invio – tramite Posta Elettronica – della carta servizi al Service Desk, da parte del Referente dell'ufficio che è l'unico titolare ad inoltrare la richiesta.

La tabella sottostante riporta l'elenco delle Carte Servizi

<b>Nome</b>	<b>Richiesta (Ulteriori dettagli sulle richieste sono indicate nelle carte servizi)</b>
CS-A1-MOD-SpostamentoPdL	Spostamento fisico di una pdl nell'ambito di uno stesso sito o tra siti diversi
CS-B1-MOD-PDLAGGIUNTIVA	Installazione di una nuova PdL secondo le configurazioni concordate
CS-E-MOD-DISTRIBUZIONE SW.DOC	Installazione/Disinstallazione software a postazioni esistenti secondo le configurazioni concordate
CS-F-MOD-RICONFIGURAZIONE_PDL.DOC	Riconfigurazione PdL secondo le configurazioni concordate a seguito di trasloco o per esigenze di ufficio
CS-G1-MOD-GESTIONEUTENZEDOMINIO.DOC	Intervento di gestione delle utenze (creazione, modifica, cancellazione di uno o più utenze)
CS-G2-MOD-EMISSIONEBADGE.DOC	Richiesta di emissione badge
CS-H-MOD-PASSWORDUTENTI_INFRASTRUTTURA.DOC	Gestione Password (reset/modifica)

Nome	Richiesta (Ulteriori dettagli sulle richieste sono indicate nelle carte servizi)
CS-I-MOD-ABILITAZIONEAPPLICAZIONE.DOC	Intervento per la gestione del profilo utente (abilitazione/disabilitazione di un servizio per uno o più utenti, abilitazione/disabilitazione all'uso delle liste di distribuzione, RAS, VPN, ...)
CS-I2-MOD-UTENZAINTERNET.DOC	Abilitazione/disabilitazione Internet
CS-I3-MOD-SERVIZISPECIFICIUTENTI_LAPTOP.DOC	Abilitazione/disabilitazione VPN/RAS
CS-I5-MOD-CAMBIPOLO_PDL.DOC	Abilitazione/disabilitazione Cambio Polo
CS-K-MOD-CREAZIONE_CANCELLAZIONEPE.DOC	Intervento per la gestione delle caselle di posta elettronica (creazione, spostamento e cancellazione utenze)
CS-K2-MOD-MIGRAZIONEUTENZAPE.DOC	Migrazione utenze PE
CS-L-MOD-UTILIZZOLISTEDISTRIBUZIONE.DOC	Gestione delle liste di distribuzione (inserimento/cancellazione di indirizzi nelle liste di distribuzione)
CS-M-MOD-SW_NOSTANDARD.DOC	Inserimento di un prodotto sw nella configurazione della PdL
CS-P-MOD-RESTOREDACARTELLAPUBBLICA.DOC	Backup e restore di dati

Le predette Carte Servizi sono pubblicate sulla Intranet, nella sezione Uffici Periferici. ([http://www.mpi.it/organizzazione\\_mpi/default.htm?uupp1](http://www.mpi.it/organizzazione_mpi/default.htm?uupp1)).