MINISTERO del LAVORO
e delle POLITICHE SOCIALI

Allegato 8 - Politica sulla Sicurezza delle informazioni

Politica

sulla sicurezza delle informazioni

MINISTERO del LAVORO
e delle POLITICHE SOCIALI

Indice

1. Finalità

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti dal Ministero del lavoro e delle politiche sociali (di seguito "Ministero" o "Amministrazione") al fine di tutelare il proprio patrimonio informativo.

La sicurezza delle informazioni è un elemento essenziale e prioritario per il perseguimento degli obiettivi di interesse pubblico propri dell'Amministrazione. Questa difatti, gestisce le informazioni nel rispetto delle leggi e dei regolamenti vigenti, in particolare nel rispetto dei principi a tutela della privacy, nonché di quelli di trasparenza, correttezza, responsabilità e sostenibilità.

L'insieme di misure organizzative, tecniche e procedurali sono messe in atto dal Ministero a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- **Riservatezza**, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- **Integrità**, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- **Disponibilità**, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Inoltre, con la presente politica si intendono formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- Preservare al meglio l'immagine del Ministero quale amministrazione affidabile e competente;
- Proteggere il patrimonio informativo dei propri utenti;
- Evitare ritardi nel rilascio dei servizi erogati;
- Rispondere pienamente alle indicazioni della normativa vigente e cogente;
- Aumentare, nei funzionari del Ministero, il livello di sensibilità e la competenza su temi di sicurezza.

2. Efficacia e ambito di applicazione

La presente politica per la sicurezza delle informazioni si applica con efficacia immediata al Ministero del lavoro e delle politiche sociali, a tutto il personale interno ed alle terze parti che collaborano alla gestione

delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

3. Definizioni ed abbreviazioni

Ai fini della presente procedura, si riportano le seguenti definizioni:

- **Direzione Generale dell'innovazione tecnologica, delle risorse strumentali e della comunicazione:** di seguito "Direzione Generale innovazione tecnologica";
- **dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);
- **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;
- **titolare del trattamento**: persona fisica o giuridica, autorità pubblica o altro organismo che determina le finalità e i mezzi del trattamento di dati personali;
- **categorie particolari di dati personali ("dati sensibili")**: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare, in modo univoco, una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- **dati personali relativi a condanne penali e reati ("dati giudiziari")**: dati che rendono identificabile la condizione di imputato o indagato dell'interessato e/o dati relativi a provvedimenti penali di condanna.

4. Dispositivi informatici

L'Amministrazione è esclusiva titolare e proprietaria dei dispositivi informatici messi a disposizione degli utenti, nonché unico esclusivo titolare e proprietario di tutte le informazioni e dati personali in essi contenuti e/o trattati; tali informazioni o dati devono essere trattati dagli utenti adottando criteri di adeguata riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta. I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità degli utenti esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle istituzionali.

I Dispositivi Informatici oggetto della presente politica sono:

- PC Desktop;
- PC Laptop;
- Smartphone.

4.1 Regole per un corretto utilizzo dei dispositivi informatici

Per un corretto utilizzo dei dispositivi informatici messi a disposizione dall'Amministrazione, è importante seguire le regole di buon uso di seguito riportate. In particolare, non è consentito:

a) modificare le configurazioni di sistema impostate dal Team del supporto tecnico del Ministero;
b) la gestione, la memorizzazione o il trattamento di file, documenti e/o informazioni personali dell'utente o comunque non afferenti alle attività lavorative;
c) installare e/o utilizzare programmi provenienti dall'esterno, salvo previa autorizzazione esplicita del Team di supporto tecnico, al fine di evitare di installare software malevolo e dunque di alterare il corretto funzionamento del dispositivo;
d) installare alcun software di cui l'Amministrazione non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul dispositivo, senza che questa sia stata certificata dal Team di supporto tecnico. È, peraltro, vietato fare copia del software installato al fine di farne un uso personale;
e) aggiungere o collegare dispositivi hardware o periferiche (es. chiavi USB) diversi da quelli consegnati, senza autorizzazione espressa del Team di supporto tecnico;
f) utilizzare directory di rete o dispositivi di archiviazione esterni differenti rispetto a quelli resi disponibili dal Team di supporto tecnico;
g) effettuare in proprio attività manutentive.

4.2 Regole per l'utilizzo dei Personal Computer (Desktop e Laptop)

Il Personal Computer (di seguito PC) consegnato agli utenti contiene tutti i software necessari a svolgere le attività previste dal proprio ruolo. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. L'accesso al PC è protetto

da password, tale password deve essere custodita dall'utente con la massima diligenza e non divulgata. Per un corretto utilizzo del PC:

a) in caso di allontanamento dalla propria postazione, attivare sempre il salvaschermo protetto da password (ctrl+alt+canc e blocca). Le postazioni di lavoro sono protette automaticamente in caso di abbandono della propria stazione di lavoro per un periodo di tempo superiore ai 10 minuti, in quanto è impostato un blocco automatico con funzionalità di salva schermo;
b) chiudere la sessione (Logout) a fine giornata;
c) spegnere il PC dopo il Logout;
d) controllare sempre che vicino alla postazione di lavoro non vi siano persone non autorizzate che possano prendere visione delle schermate del PC;
e) non dare accesso al proprio computer ad altri utenti, a meno che siano utenti con cui si condivide l'utilizzo dello stesso PC o a meno di necessità stringenti e sotto il proprio costante controllo.

4.3 Regole per l'utilizzo dei Dispositivi Mobili (Smartphone)

Ad ogni utente che abbia una mansione per la quale è stato ritenuto necessario l'utilizzo di uno Smartphone, viene assegnata una SIM ed un dispositivo di marca e modello tra quelli prescelti dall'Amministrazione. In caso di cessazione del rapporto di lavoro per qualsiasi causa o qualora vengano meno i requisiti di assegnazione (sia per un cambiamento della politica che per un mutamento delle mansioni assegnate al dipendente), l'assegnatario è tenuto a riconsegnare il dispositivo c/o il Team di supporto tecnico. Ciascun utente è tenuto a rispettare le seguenti regole di utilizzo per i dispositivi mobili:

a) i dispositivi mobili sono strumenti di lavoro, non personali, del quale l'affidatario è responsabile, questi devono essere adoperati esclusivamente per scopi connessi alla mansione;
b) per motivi di sicurezza è necessario impostare sempre sul dispositivo:
    - all'accensione: il PIN della SIM;
    - al blocco schermo per inattività: il PIN/password che viene richiesto all'accensione o il riconoscimento biometrico (es: impronta digitale);
c) è possibile installare software (APPS) oltre quello già presente sul dispositivo al momento della consegna solo per finalità lavorative;

d) per i dispositivi mobili che sono dotati di connessioni WiFi e Bluetooth l'utilizzo di queste connessioni è regolamentato come segue:
    - non è consentito connettersi a reti WiFi delle quali non si conosce l'origine;
    - la connessione deve essere eseguita esclusivamente verso reti note, sulle quali siano certificabili le modalità di accesso anche se in ambito pubblico e/o privato;
    - è consigliabile disattivare le connessioni WiFi e Bluetooth quando non più necessarie per evitare consumi eccessivi della batteria del dispositivo e problemi di sicurezza;
e) non spostare la SIM su altri device (es. privati) non autorizzati;
f) provvedere al backup dei dati salvati sul dispositivo mobile prima di chiederne il ripristino.

4.4 Restituzione dei dispositivi

Ogni dispositivo ed ogni memoria esterna affidati agli utenti, al termine del loro utilizzo dovranno essere restituiti al Team di supporto tecnico, che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento. In particolare, l'Amministrazione, dove previsto, provvederà a cancellare o a rendere inintelligibili i dati memorizzati negli stessi.

In caso di perdita o furto di un Dispositivo Mobile o Laptop al di fuori degli spazi aziendali, deve far seguito la denuncia alle autorità competenti. Inoltre, è necessario avvisare immediatamente:

a) il proprio responsabile;
b) il Team di supporto tecnico che provvederà ad occuparsi delle procedure connesse a sicurezza e privacy.

A seguito della cessazione del rapporto lavorativo, o comunque, al venir meno della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, gli utenti sono tenuti a seguire le seguenti indicazioni:

a) procedere tempestivamente alla restituzione dei dispositivi in uso;
b) è fatto assoluto divieto di formattare, alterare, manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti;

c) al momento della restituzione del dispositivo aziendale, se richiesto, gli utenti devono rimuovere eventuali meccanismi di protezione o password configurate al fine di consentire l'accesso al dispositivo al Team di supporto tecnico.

5. Password

L'accesso alla rete aziendale, al PC e agli applicativi avviene attraverso la fornitura, ad ogni utente abilitato, di uno o più identificativi utente (account) e password. Gli identificativi utente sono univoci e personali.

L'utente non deve divulgare e/o trasferire nessuno degli account a lui affidati (tantomeno le password), poiché le attività e le abilitazioni sui sistemi sono specifiche per ogni singolo account, per cui l'utente è responsabile di tutte le attività eseguite mediante gli account a lui forniti. Il mantenimento della sicurezza dei sistemi informatici dipende anche dal modo in cui gli utenti si adoperano per proteggere tali credenziali. Ogni utente ha infatti la responsabilità di utilizzare i meccanismi e le procedure di sicurezza in modo da proteggere il proprio lavoro e i propri dati. Per questo motivo è necessario porre particolare attenzione alla scelta della password e della protezione e custodia della stessa.

Per una corretta e sicura gestione delle proprie password, l'utente è tenuto a procedere alla modifica della password al primo utilizzo e, successivamente, almeno ogni 3 mesi. La Direzione Generale dei sistemi informativi, dell'innovazione tecnologica, del monitoraggio dati e della comunicazione (ora DG dell'innovazione tecnologica, delle risorse strumentali e della comunicazione per effetto del DPCM n. 140/2021) è intervenuta prescrivendo delle specifiche regole di formato nell'individuazione delle password, al fine di elevare i requisiti di sicurezza nell'accesso alle risorse di rete dell'Amministrazione. Nel dettaglio, la password dovrà rispettare dei requisiti minimi:

- Non potrà contenere parti significative del nome di account o del nome dell'utente;
- Dovrà essere composta almeno da 8 caratteri;
- Dovrà contenere caratteri appartenenti a tre delle quattro categorie seguenti:
  - ❖ Lettere maiuscole (da A a Z)
  - ❖ Lettere minuscole (da a a z)
  - ❖ I primi 10 numeri di base (da 0 a 9)
  - ❖ Caratteri speciali (ad esempio $, #, %)

Per una corretta gestione delle password, ogni utente deve attenersi alle seguenti indicazioni:

a) le credenziali di autenticazione devono essere custodite e non rese note a colleghi o soggetti esterni;
b) in nessun caso devono essere annotate password in chiaro, sia su supporti cartacei che elettronici;
c) qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a cambiarla;
d) si consiglia di non utilizzare le opzioni di "compilazione automatica" o "remember password", disponibili nei browser o in altre applicazioni;
e) la password non deve essere basata su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa;
f) evitare di digitare la propria password in presenza di altri soggetti in grado di vedere la tastiera, anche se collaboratori o dipendenti dell'Amministrazione;
g) non utilizzare per scopi privati (es. social, newsletter private) password adottate per applicativi del Ministero.

6. Antivirus

I virus, come qualsiasi altra forma di software malevolo, possono essere trasmessi tramite download di file via internet, via mail, scambio di supporti removibili, *file sharing*, chat etc. Per proteggere l'Amministrazione dall'azione e diffusione di *malware e virus*, il Team di supporto tecnico provvede ad installare e attivare su tutte le postazioni di lavoro il sistema Antivirus, in grado di aggiornarsi automaticamente con frequenza almeno quotidiana.

L'Utente, da parte sua, è tenuto a comunicare al Team di supporto tecnico:

a) eventuali anomalie o malfunzionamenti riscontrati del sistema Antivirus;
b) eventuali segnalazioni relative alla presenza di virus o file sospetti.

Inoltre, si rende noto che:

a) è vietato accedere alla rete dell'Amministrazione senza servizio antivirus attivo e aggiornato sulla propria postazione;
b) è vietato ostacolare l'azione dell'antivirus;

c) è vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Amministrazione, anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
d) è vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail ricevute da persone conosciute ma con testi non canonici o in qualche modo difformi dal normale.

Qualora l'utente rilevi un virus sul proprio computer o se ne sospetti la presenza, è bene seguire la seguente procedura:

1. scollegare il proprio computer dalla rete;
2. informare immediatamente il Team di supporto tecnico;
3. se possibile, identificare e segnalare altri utenti potenzialmente esposti al virus.

7. Internet

La navigazione Internet è un servizio che l'Amministrazione rende disponibile per finalità lavorative a determinati soggetti in relazione all'attività svolta. Il Ministero adotta idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e *blacklist*. A tutela della sicurezza delle risorse informatiche, è fatto divieto all'utente di:

a) accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, delle disabilità;
b) scaricare software non autorizzato (anche gratuito) prelevato da siti Internet;
c) registrarsi, utilizzando l'indirizzo mail aziendale, a siti i cui contenuti non siano legati all'attività lavorativa;
d) partecipare a forum non professionali, utilizzare chat line per scopi privati, lasciare commenti ad articoli o iscriversi a mailing list spendendo la denominazione del Ministero;
e) memorizzare documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
f) promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica del Ministero;

g) creare siti web personali sui sistemi dell'Amministrazione.

Ogni eventuale navigazione di questo tipo, comportando un utilizzo illegittimo di Internet, nonché un possibile illecito trattamento di dati personali e di categorie particolari di dati personali, è posta sotto la personale responsabilità dell'utente inadempiente.

8. Posta Elettronica

L'utilizzo della posta elettronica è connesso allo svolgimento dell'attività lavorativa; pertanto è da evitare l'utilizzo della posta elettronica per motivi personali.

Gli utenti hanno in utilizzo indirizzi nominativi di posta elettronica. Possono essere assegnate anche caselle e-mail con natura impersonale (ad esempio info, amministrazione, direzione); in questi casi, è preferibile evitare che il destinatario delle mail possa considerare l'indirizzo assegnato come "privato".
L'utilizzo della posta elettronica deve essere effettuato dall'utente con la massima diligenza, applicando i seguenti principi:

a) è vietato creare, archiviare o spedire, anche solo all'interno della rete interna, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, o in genere a pubblici dibattiti utilizzando l'indirizzo fornito dal Ministero;
b) è vietato configurare inoltri automatici verso caselle di posta non gestite dall'Amministrazione;
c) i messaggi contenenti allarmi su virus o "*malicious code*" devono essere inoltrati, senza aprire eventuali allegati, esclusivamente all'indirizzo di posta elettronica del Team di supporto tecnico;
d) è vietato inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
e) non è consentito diffondere all'esterno indirizzi di posta elettronica diversi dal proprio senza il consenso dei rispettivi titolari;
f) non è consentito inviare a destinatari non appartenenti al personale dipendente, ed anche utilizzando canali telematici non protetti, informazioni riservate in chiaro e/o concernenti dati personali di natura sensibili.

Gli utenti devono, inoltre, tener presente che, nell'assolvimento dei propri compiti, il personale del Team di supporto tecnico può avere, saltuariamente, la necessità di analizzare i dati transazionali dei messaggi di posta per garantire il corretto funzionamento del servizio e in queste occasioni è possibile che avvengano inavvertitamente accessi al contenuto stesso dei messaggi. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora si verificassero i casi citati.

8.1 Phishing

Il *Phishing* è un tipo di frode, veicolata principalmente tramite la posta elettronica, attraverso la quale un malintenzionato cerca di ingannare la vittima inconsapevole convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile o una persona nota all'interno di una comunicazione digitale.

Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale. Per evitare di incorrere in questa tipologia di truffa, è bene attenersi sempre ai seguenti accorgimenti:

a) verificare sempre il vero indirizzo del mittente, di solito riportato vicino al nome;
b) non rispondere mai alle e-mail sospette;
c) non cliccare mai sui link proposti all'interno di mail sospette. Contattare eventualmente l'ente coinvolto che sembra richiedere le informazioni;
d) prestare massima cautela ed attenzione nell'apertura degli allegati presenti all'interno di mail sospette.

Il Team di supporto tecnico ha già provveduto a mettere in atto tutte le azioni raccomandate per evitare impatti sui sistemi, in ogni caso la collaborazione e attenzione dell'utente è fondamentale.
In caso di dubbi e per verifica è possibile inoltrare le mail sospette alla casella mail spam@lavoro.gov.it.

9. Uso delle stampanti

All'interno delle sedi del Ministero sono presenti una serie di stampanti condivise in rete tra gli utenti, allo scopo di assicurare un alto livello di qualità delle stampe, ottimizzando i costi.

I documenti che passano attraverso le stampanti contengono numerose informazioni, spesso confidenziali, e dati personali che devono essere protetti e resi sicuri. Al fine di minimizzare il rischio di diffusione non autorizzata di informazioni la Direzione Generale dei sistemi informativi, dell'innovazione tecnologica, del

monitoraggio dati e della comunicazione (ora DG dell'innovazione tecnologica, delle risorse strumentali e della comunicazione per effetto del DPCM n. 140/2021) ha installato un dispositivo per la lettura dei badge sulle stampanti.

Il nuovo dispositivo installato consentirà di avviare le stampe esclusivamente attraverso il badge personale in uso. Pertanto, l'utente invierà il documento in stampa e il dispositivo rilascerà i documenti solo quando il mittente avrà effettuato il log-in con il proprio badge. In tal modo solo le persone autorizzate possono accedere ai documenti, stamparli o effettuare scansioni.

10. Accesso remoto

Allo scopo di consentire lo svolgimento delle normali attività lavorative agli Utenti che si trovano fuori sede, l'Amministrazione mette a disposizione un servizio di accesso remoto sicuro, detto "collegamento VPN".

Il servizio è gestito dal Team di supporto tecnico, al quale ci si deve rivolgere per richiedere le necessarie abilitazioni e configurazioni per l'accesso VPN.

L'accesso è garantito dall'utilizzo di hardware e software standard messi a disposizione dal Ministero. Non è possibile eseguire l'accesso alla rete in altro modo. L'accesso è inteso solo e soltanto per il personale autorizzato esplicitamente, per cui non è assolutamente consentito fornire le proprie credenziali di accesso remoto a terzi. L'Utente è responsabile delle credenziali di accesso e del materiale che gli è fornito per eseguire l'accesso.

11. Sistemi e Servizi in Cloud

Per tutti i servizi in Cloud resi disponibili e approvati dall'Amministrazione, ne è concesso il pieno utilizzo agli utenti, per tutti e soli gli scopi previsti per lo svolgimento dell'attività lavorativa.

Non è consentito agli utenti l'utilizzo dei sistemi o piattaforme Cloud, diverse da quelle adottate dall'Amministrazione, per finalità personali e/o per condivisione di informazioni (*file sharing e collaboration*) con entità interne o esterne.

12. Clean Desk Policy

Gli utenti sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti cartacei.

Gli utenti sono invitati ad adottare una "politica della scrivania pulita" (Clean Desk Policy), ovvero si richiede di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali.
È opportuno che gli archivi fisici di dati aziendali, in particolari gli archivi contenenti dati personali, di tipo "sensibili" e/o "giudiziari" (v. sezione "Definizioni ed abbreviazioni"), ai sensi della normativa sulla privacy, siano conservati in contenitori dotati di chiave (armadi, cassettiere, schedari) e, nel caso di allontanamento temporaneo del lavoratore dalla propria postazione di lavoro, gli stessi non devono essere lasciati incustoditi.
Inoltre, gli utenti possono accedere ai soli archivi di propria competenza e devono attenersi a quanto segue:

- l'accesso è permesso per il tempo necessario allo svolgimento delle proprie mansioni;
- la documentazione eventualmente prelevata deve essere riposta negli archivi di provenienza al termine delle operazioni di trattamento;
- i documenti contenenti dati personali devono essere conservati con cura;
- i documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'Amministrazione;
- i documenti contenenti dati sensibili o giudiziari devono essere custoditi fino alla restituzione in modo da evitare l'accesso agli stessi dati a persone prive di autorizzazione.

13. Controllo

Nel rispetto delle normative vigenti, l'Amministrazione, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

a) tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
b) evitare il verificarsi di illeciti o per esigenze di carattere difensivo anche preventivo;
c) verificare la funzionalità del sistema o dei dispositivi Informatici.