DISCIPLINARE PER L' UTILIZZO DI PERSONAL COMPUTER, DISPOSITIVI ELETTRONICI AZIENDALI, POSTA ELETTRONICA E INTERNET

INDICE

1. Premesse

L'esigenza dell'Ires Piemonte di adottare un Disciplinare per l'utilizzo dei personal computer fissi e portatili, dei dispositivi elettronici aziendali in generale (quali a titolo esemplificativo ma non esaustivo fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari aziendali, pen drive e supporti di memoria), della posta elettronica e internet (di seguito il "Disciplinare") nasce dal ricorso sempre più frequente dell'utilizzo di tali strumenti nell'organizzazione e nell'espletamento dell'attività lavorativa. In applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., l'utilizzo di tali indispensabili risorse deve avvenire nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo tra l'Ente e i propri dipendenti e adottando tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non avveduto di tali strumenti può condurre, anche in considerazione della difficoltà di tracciare una netta linea di confine tra l'attività lavorativa e la sfera personale e la vita privata del lavoratore e dei terzi che interagiscono con quest'ultimo.

In tale contesto, il Garante ha emanato la Deliberazione n. 13 del 1° marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" (reperibile presso: **http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522**), con la quale ha inteso prescrivere ai datori di lavoro alcune misure per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.

Il presente Disciplinare, pertanto, è adottato al fine di richiamare le indicazioni e le misure necessarie e opportune per disciplinare il corretto utilizzo nel rapporto di lavoro dei personal computer (fissi e portatili), dei dispositivi elettronici aziendali in generale, della posta elettronica e di Internet, definendone le modalità di utilizzo nell'ambito dell'attività lavorativa.

2. Adozione del Disciplinare e sua efficacia

Il Disciplinare è stato redatto dall'Amministratore di sistema dell'IRES.

I dipendenti saranno informati tramite apposita circolare e il Disciplinare sarà reso disponibile anche sul sito intranet dell'Istituto.

Il Disciplinare potrà essere aggiornato ogniqualvolta se ne presenti l'opportunità e di tali revisioni sarà data tempestiva comunicazione ai dipendenti.

Le disposizioni contenute nel Disciplinare si applicano a tutti i dipendenti dell'Ires Piemonte, nonché a tutti i soggetti rispetto ai quali verranno espressamente riconosciute applicabili, ad esempio facendo riferimento al presente Disciplinare nei relativi contratti (es. collaboratori esterni, stagisti, borsisti, consulenti).

E' responsabilità di tutti i soggetti che utilizzano il personal computer ed altri dispositivi elettronici, la posta elettronica e internet messi a disposizione dall'Istituto, applicare e rispettare puntualmente le disposizioni del presente Disciplinare. Fermo restando quanto previsto dalle seguenti fonti:

- -D.Lgs. 30 giugno 2003, n. 196 " Codice in materia di protezione dei dati personali";

- Linee guida del Garante per la Protezione dei Dati personali per posta elettronica e internet.

- (Deliberazione n. 13 del 1 marzo 2007);

- Contratti collettivi nazionali per i dipendenti del comparto Regioni/Enti locali, categorie e per i dipendenti di Area Dirigenziale e rispettivi contratti collettivi decentrati integrativi per il personale dell'Ires Piemonte;

- Statuto dei Lavoratori;

- il contenuto del presente Disciplinare costituisce, per i dipendenti, disposizione di servizio e deve considerarsi integrativo di quanto previsto da: informative in materia di trattamento dei dati personali rilasciate ai dipendenti ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali;
- lettere di incarico destinate a responsabili e incaricati e le relative istruzioni ivi contenute;
- così come qualsiasi altra prescrizione in materia di privacy.

3. **Principi generali**

Il Disciplinare è adottato per assicurare la funzionalità e il corretto impiego dei personal computer fissi e portatili, dei dispositivi elettronici aziendali in generale, della posta elettronica e di internet da parte dei lavoratori: a tale fine, definisce le modalità d'uso di tali strumenti nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali.

Le disposizioni e le prescrizioni qui indicate vanno affiancate e integrano quelle già previste nel Documento Programmatico per la Sicurezza ("DPS"), nel contratto di lavoro e, in generale, nelle disposizioni pattizie o regolamentari vigenti.
Il luogo di lavoro è una formazione sociale nella quale è assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Costituzione, Art. 2087 c.c., art. 2, comma 5, Codice dell'amministrazione digitale, D.Lgs. 7 marzo 2005, n. 82).

Le regole che disciplinano l'utilizzo del personal computer, dei dispositivi elettronici aziendali, della posta elettronica e di internet si conformano, pertanto, ai seguenti principi generali:

- Principio di necessità (ex art. 3 Codice in materia di protezione dei dati personali).

I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi ed opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

- Principio di correttezza (ex art. 11, comma 1, lett. a Codice in materia di protezione dei

dati personali).

Le caratteristiche essenziali del trattamento sono rese note ai lavoratori. Ciò assume particolare rilievo nel caso di trattamenti di dati acquisiti dall'elaborazione di informazioni relative alla corrispondenza elettronica, poiché un simile trattamento postula necessariamente il ricorso a tecnologie dell'informazione che, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa.

- Principio di determinatezza e legittimità delle finalità del trattamento (ex art. 11, comma 1 lett. b del Codice in materia di protezione dei dati personali).

- Principio di pertinenza e non eccedenza.

Il datore di lavoro deve trattare i dati nella misura meno invasiva possibile.

- Principio di trasparenza.

Tale principio si accompagna ed è coerente con quanto previsto dall'art 4, comma 2, dello Statuto dei lavoratori secondo cui "è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna". Tramite la sua applicazione si esclude la possibilità del controllo informatico all'insaputa dei lavoratori.

4. Regole relative all'utilizzo della postazione di lavoro (PC), dei personal computer portatili e dei dispositivi elettronici aziendali.

I personal computer fissi e portatili e i programmi per elaboratore su di esso installati sono uno strumento di lavoro e contengono dati riservati e informazioni personali di terzi ai sensi della legge sulla privacy: vanno, pertanto, utilizzati e conservati, insieme ai relativi documenti esplicativi, con diligenza e cura, attenendosi alle prescrizioni fornite dal datore di lavoro e nel rispetto delle indicazioni da questo fornite.

Le impostazioni dei personal computer e dei relativi programmi per elaboratore installati sono predisposte dall'amministratore di sistema sulla base di criteri e profili decisi dalla Direzione dell'Istituto, in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dalla Direzione stessa. Il dipendente non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione da parte della Direzione.

L'installazione sui personal computer dei dipendenti di sistemi operativi e programmi applicativi e, in generale, di software, avviene ad opera dell'Amministratore di sistema, che opera seguendo i necessari criteri di sicurezza. L'uso di tali programmi deve avvenire nel rispetto dei contratti di licenza che li disciplinano e delle specifiche prescrizioni di volta in volta indicate.

L'installazione di programmi da parte del dipendente, ove sia consentito dal proprio personal computer e dalle relative impostazioni, deve avvenire senza aggirare divieti o restrizioni eventualmente previsti, nel pieno rispetto delle condizioni che disciplinano l'utilizzo di tali programmi e, in generale, della normativa vigente, con particolare riferimento alle disposizioni in materia di protezione di diritti di proprietà intellettuale: abusi o utilizzi illeciti saranno puniti conformemente alle disposizioni che disciplinano il rapporto di lavoro. In ogni caso, il dipendente sarà responsabile e sarà chiamato a manlevare e tenere indenne l'Amministrazione Regionale da qualsiasi danno o richiesta di risarcimento che venga avanzata da soggetti terzi.

Tutti i software caricati sul sistema operativo ed in particolare i software necessari per la protezione dello stesso o della rete internet quali antivirus antispyware ecc.) non possono essere disinstallati o in nessun modo manomessi dai dipendenti, (salvo quando questo sia richiesto dall'amministratore di sistema per compiere attività di manutenzione o aggiornamento.

L'accesso al personal computer, ai programmi applicativi e alle varie funzionalità messe a disposizione dei dipendenti per lo svolgimento dell'attività avviene previa autenticazione, che consiste nella verifica dell'identità del dipendente attraverso l'uso di un codice identificativo e di una parola chiave (password).

Scelta, custodia, modifica e utilizzo della password devono rispettare le prescrizioni contenute nel Documento Programmatico sulla Sicurezza. Si ricorda, a tale riguardo, che:

- al primo accesso ad un sistema e/o ad una banca dati, il dipendente ha la responsabilità di cambiare la password assegnatagli dall'Amministratore di Sistema. Tale password deve essere al minimo lunga otto caratteri ed includere sia cifre sia lettere;

- il dipendente è obbligato dal sistema a cambiare la propria password su base almeno semestrale, non riutilizzando password precedentemente usate ed evitando di adottare password "banali" (il nome dei figli, la propria data di nascita, la targa della propria auto, etc.);

- il dipendente ha la responsabilità di custodire con diligenza la propria password (ed i dispositivi fisici eventualmente in suo possesso). In nessuna circostanza il dipendente è autorizzato a condividere le proprie credenziali di autenticazione (User-Id, password e smart-card) con altri incaricati o terze persone, fatto salvo quanto più avanti previsto in caso di assenza o impossibilità del dipendente;

- l'amministratore di Sistema ha la responsabilità di assicurare che la componente pubblica delle credenziali di autenticazione (il "codice utente" o User-Id) non sia più riutilizzata per identificare altri dipendenti o comunque altri utenti del sistema, neanche in tempi diversi o successivi.

Sono fatte salve tutte le prescrizioni ulteriori previste per il trattamento dei dati sensibili o giudiziari.

In caso di furto o smarrimento della smart card, o comunque in tutti i casi in cui il dipendente abbia fondati motivi di ritenere che ne possa essere stato fatto un utilizzo da

parte di terzi, il dipendente deve darne informazione senza alcun indugio. Il dipendente dovrà ugualmente informare l'Amministrazione nel caso in cui, per qualsiasi motivo, abbia fondati motivi di ritenere che possa essere compromessa la riservatezza della password, o comunque che ne sia stato fatto un utilizzo indebito.

In caso di allontanamento anche temporaneo dalla stazione di lavoro (personal computer fisso o portatile), il dipendente non deve lasciare il sistema operativo aperto con la propria password e/o smart card inserita. Al fine di evitare che persone estranee effettuino accessi non permessi, il dipendente deve attivare il salvaschermo con password o deve bloccare il computer (utilizzando i tasti CTRL+ALT+CANC).

I codici identificativi, e le password dei dipendenti saranno disattivate nel caso in cui i dipendenti cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa.

Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare a un altro dipendente a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare al responsabile dell'area in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.

In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, ed il dipendente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, il responsabile della struttura a cui è assegnato il dipendente può richiedere con apposita e motivata richiesta all'Amministratore del Sistema di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il responsabile della struttura deve informare il dipendente dell'avvenuto accesso appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

Per finalità di assistenza, manutenzione e aggiornamento e previo consenso esplicito del dipendente stesso, l'amministratore di sistema potrà accedere da remoto al personal computer del dipendente attraverso un apposito programma software.

L'Amministratore di Sistema effettuerà, inoltre, attività di monitoraggio e verifica dell'efficacia delle protezioni predisposte sul sistema informativo rispetto ad aggressioni esterne senza che siano necessarie preventive ulteriori informative. Le risultanze di tali attività di monitoraggio e verifica potranno essere utilizzare soltanto in modo proporzionato e pertinente alle finalità e alla natura delle stesse (e non, ad esempio, al fine di attuare indirettamente un controllo a distanza dell'attività lavorativa svolta dal dipendente).

Al fine di garantire la disponibilità dei documenti di lavoro assicurandone il backup giornaliero, il dipendente dovrà procedere al loro salvataggio su supporti fisici quali hard disk esterni e/o chiavette usb così come indicato dall'Autorità Garante con il provvedimento a carattere generale del 1 marzo 2007 'Linee guida del Garante su posta elettronica e internet'.

Il dipendente è tenuto ad osservare le medesime precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti i dispositivi elettronici aziendali di cui fa uso, tra cui ad esempio fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari aziendali, pen drive e supporti di memoria.

In particolare i supporti di memoria portatili e comunque riutilizzabili dovranno essere custoditi con la massima cura ed utilizzati adottando le necessarie cautele affinché soggetti estranei non possano venire a conoscenza dei documenti e delle informazioni ivi contenute.

In generale tutti i dispositivi elettronici aziendali sono forniti al dipendente per lo svolgimento della sua attività lavorativa, nell'ambito delle mansioni a questo affidate. L'uso per fini personali è da considerare pertanto eccezionale e limitato a comunicazioni occasionali e di breve durata, ad esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali.

5. **Regole applicabili all'utilizzo di internet**

La rete internet può e deve essere utilizzata dal dipendente a supporto all'attività lavorativa.

Pertanto si ricorda al dipendente di utilizzare la rete internet nel rispetto delle leggi vigenti e prestando particolare cautela al fine di non importare virus, spam o altri programmi informatici dannosi.

6. **Regole applicabili all'utilizzo di posta elettronica**

La casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa.

Si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica assegnati dall'Ires per le comunicazioni personali.

Le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.

I messaggi di posta elettronica devono contenere un avvertimento ai destinatari del seguente tenore letterale: "Il presente messaggio contiene informazioni di natura professionale attinente all'attività lavorativa. Ai fini dello svolgimento dell'attività lavorativa le eventuali risposte potranno essere conosciute da altri soggetti nell'ambito dell'organizzazione del mittente. Questo messaggio di posta elettronica e il suo contenuto sono riservati e confidenziali e destinati esclusivamente al soggetto indicato nell'indirizzo.

Se per errore ricevete questo messaggio o non siete il soggetto destinatario o delegato dal destinatario alla lettura, Vi preghiamo di darcene immediatamente notizia e quindi di cancellare definitivamente il messaggio di posta elettronica".

In caso di assenza prolungata programmata del dipendente, si consiglia e si raccomanda al dipendente di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate di un collega o della struttura di riferimento che può essere contattata in sua assenza e/o altre modalità utili di contatto della struttura organizzativa.

Nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare un altro dipendente a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare al responsabile dell'area in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.

In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, ed il dipendente non abbia delegato un altro dipendente (fiduciario), secondo quanto sopra specificato, il responsabile della struttura cui afferisce il dipendente può richiedere all'Amministratore del Sistema di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il responsabile della struttura deve informare il dipendente appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

Nel caso in cui il dipendente non presti più la sua attività lavorativa presso l'Ires Piemonte, la casella di posta elettronica sarà prontamente disattivata.

Così come indicato dall'Autorità Garante con il provvedimento a carattere generale del 1° marzo 2007 'Linee guida del Garante su posta elettronica e internet'.

Qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente l'amministratore di sistema.

7. **Controlli effettuati dall'Istituto**

L'IRES PIEMONTE si riserva di effettuare controlli per verificare il rispetto del Disciplinare. Rispetto a tali controlli il presente Disciplinare costituisce preventiva e completa informazione nei confronti dei dipendenti.

Qualora venga constatata la violazione del presente Disciplinare, l'IRES potrà irrogare le sanzioni applicabili previste dai contratti collettivi vigenti, nel rispetto delle procedure stabilite dagli stessi contratti.

Oltre a ciò, l'Amministratore di Sistema si riserverà di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

Oltre a tali controlli di carattere generale, l'Amministratore di Sistema si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazione di attività che hanno causato danno all'amministrazione, che ledono diritti di terzi o che , comunque, sono illegittime.

Inoltre, si rammenta che, conformemente a quanto previsto dal Documento Programmatico sulla Sicurezza e in osservanza della vigente normativa, i dati relativi all'utilizzo della posta elettronica e di internet sono conservati per periodi di tempo strettamente limitati, secondo le modalità e le tempistiche indicate nello stesso Documento Programmatico.