

**ADDENDUM all'Accordo del 10 maggio 2005
riguardante l'Adempimento delle previsioni dell'art. 4, comma 2
della L. 300/70 (Statuto dei Lavoratori)**

IBM Italia S.p.A. (di seguito denominata anche IBM e/o Azienda) nelle persone dei sigg. Fabio Mariano e Flavia Gasbarri, Mario Bertucca, Alberto Iorio.

E

Coordinamento Nazionale delle RSU IBM Italia S.p.a. (di seguito denominato anche Coordinamento) nelle persone dei sigg. Francesco Fiaccadori, Roberto Reymond e Pier Fortunato Botton

fermo restando quanto normato dall'accordo sindacale citato in epigrafe e da intendersi qui interamente richiamato, Le parti a seguito di un esame approfondito concordano quanto segue:

- a. Vengono definiti "Privileged User" (di seguito, PU) i dipendenti che, essendo abilitati a intervenire sui sistemi dell'Azienda stessa o di terzi a un livello più elevato dell'utente comune, ricevono da IBM formale comunicazione scritta della propria definizione, in cui viene specificato l'ambiente tecnologico e operativo a cui la definizione si applica: Hardware, Sistema Operativo, Partizione (se in presenza di partizioni multiple).
- b. Che l'Accordo sull'adempimento delle previsioni dell'art. 4, comma 2, della L. 300/70 (Statuto dei Lavoratori) del 10 maggio 2005 (di seguito "Accordo") si applica ai sopradefiniti PU con le seguenti modalità:
 - I. La procedura di controllo effettuata sul dispositivo tecnologico assegnato ai PU, così come definito al punto a, avviene secondo i criteri stabiliti ai successivi punti IV, V, VI secondo i test riportati nell'ALLEGATO A.
 - II. In riferimento al punto precedente ogni qual volta si rendesse necessario un aggiornamento della procedura di controllo prevista dalla normativa sulla sicurezza (Security and Use Standards for IBM employee ITCS 300), la CCD potrà richiedere ad IBM informazioni in merito a tale aggiornamento e, qualora individuasse specificità della procedura che richiedano un esame approfondito, lo comunicherà al RARC che avvierà tempestivamente il citato esame.
 - III. L'Azienda può effettuare controlli solo seguendo la procedura di controllo dei punti IV, V, VI relativamente ai test indicati nell'ALLEGATO A; ogni altro controllo sull'attività dei PU ricade nelle modalità ordinarie previste dall'Accordo.
 - IV. I PU controllandi devono essere scelti in modo casuale, ovvero con l'applicazione di sistemi di selezione automatica riferiti alla collettività o a gruppi di lavoratori e,



Handwritten signatures of the representatives of IBM Italia S.p.A. and the Coordinamento Nazionale delle RSU.

in ogni caso, nel pieno rispetto dei principi sanciti dall'art. 6 della Legge 300/70 (Statuto dei Diritti dei Lavoratori).

- v. Il PU controllando riceve una comunicazione scritta che lo avvisa del controllo a cui sta per essere sottoposto e lo informa della procedura di controllo. Il PU controllando può richiedere l'assistenza della CCD, o di un rappresentante della RSU della propria sede, durante la procedura di controllo.
- vi. A controllo effettuato, qualora fossero rilevate irregolarità, al PU sarà comunicata la possibilità di avvalersi dell'assistenza della CCD o di un rappresentante della RSU della propria sede; in ogni caso, gli dovrà essere garantita la completa disponibilità delle informazioni inerenti al controllo. Nel caso di rilievo di irregolarità dovranno essere garantiti i diritti previsti dal punto 2f dell'Accordo.

IBM e Coordinamento confermano che l'accesso in internet ai siti sindacali continuerà ad essere assolutamente libero, legittimo e non necessitante di autorizzazione alcuna.

Segrate/Roma, 24 ottobre 2014

Letto, confermato e sottoscritto.

P. la Società






P. Il Coordinamento RSU

IBM Italia Spa





ALLEGATO A

Controlli effettuabili sul dispositivo tecnologico assegnato al PU, così come definiti nel punto a del presente Addendum, in aggiunta a quanto previsto al punto 2b dell'Accordo:

1) Controllo su Browser Internet

Tipologia controllo	sulla History del pc. Viene lanciata una procedura sul PC del dipendente che produce un Report con la lista dei Siti Visitati
Scopo del controllo	Controllare se i siti visitati sono inerenti all'attività lavorativa
Presenza Log con identificativo utente	Solo sul pc del PU
Criteri con cui dati e log sono conservati/cancellati	I log devono essere conservati per 90 giorni

2) Controllo sulle applicazioni scaricate dal dipendente

Tipologia controllo	Sull'ambiente del sistema del pc del PU. Viene lanciata una procedura sul PC del dipendente che produce un Report con la lista del SW installato.
Scopo del controllo	Controllare se le applicazioni sono inerenti all'attività lavorativa e il loro utilizzo è approvato dalle policy aziendali IBM.
Presenza Log con identificativo utente	No
Periodo preso in esame per il controllo	90 giorni prima del controllo

3) Controllo sulla USB History

Tipologia controllo	La history dei dispositivi collegati la si ottiene attraverso le funzionalità del sistema operativo host. Viene lanciata una procedura sul PC del dipendente che produce un Report con la lista dei dispositivi collegati
Scopo del controllo	Verificare i dispositivi che vengono collegati alle porte USB dei pc per identificare se l'utente utilizza propri dispositivi personali
Presenza Log con identificativo utente	No
Periodo preso in esame per il controllo	90 giorni prima del controllo

4) Controllo per verificare presenza di musica, foto e filmati sul pc del dipendente

Tipologia controllo	Sui folder del pc del dipendente. Viene lanciata una procedura sul PC del dipendente che produce un Report con la lista dei documenti in oggetto, presenti sul PC del dipendente
Scopo del controllo	Verificare che non siano presenti file personali sul pc del dipendente
Presenza Log con identificativo utente	No
Periodo preso in esame per il controllo	90 giorni prima del controllo

Alh Loni [Signature] [Signature] [Signature] [Signature]

[Signature] [Signature] [Signature]