ROMA

Dipartimento Innovazione Tecnologica

Utilizzo delle postazioni di lavoro in uso presso gli uffici di Roma Capitale

Manuale

Perché questo Manuale?
Atti di Roma Capitale

- DGC 208 30/6/2015 *"Linee guida per la predisposizione del programma strategico di ottimizzazione dei servizi di Desktop Fleet Management. Approvazione del Piano di azioni operative per la razionalizzazione dei servizi di Desktop Fleet Management"*
- DGC 356 28/10/2015 *"Approvazione del Piano strategico triennale dell'ICT di Roma Capitale e delle relative azioni operative per la razionalizzazione della spesa nel triennio 2016-2018"*

Riferimenti normativi

- artt. 2104 e 2105 Codice Civile
- art. 23 CCNL
- Statuto dei lavoratori
- D.Lgs. n. 196/2003 (Testo Unico in materia di protezione dei dati personali)
- Disposizioni in materia di Privacy e di misure minime di sicurezza (disciplinare tecnico allegato al D.Lgs. 196/2003)

Principali novità introdotte dagli atti di indirizzo

1. la riduzione delle dimensioni del parco di apparecchiature informatiche periferiche
2. l'evoluzione della modalità di stampa da servizio individuale a servizio condiviso
3. la sperimentazione di tecnologie innovative (cloud computing)
4. l'analisi dettagliata dell'utilizzo delle postazioni e dei software di base con segmentazione dell'utenza in base all'utilizzo stesso, con il coinvolgimento di tutte le strutture capitoline

Indicazioni operative

Le indicazioni del presente Manuale, in materia di trattamento dei dati personali, non sostituiscono ma integrano, se del caso, le specifiche istruzioni che vanno fornite a tutti gli incaricati (D.Lgs. 196/03 e s.m.i.) da parte del datore di lavoro, individuato nel Direttore della struttura di appartenenza.

Il Personal Computer è affidato al dipendente quale strumento di lavoro.

In caso di assegnazione del dipendente ad altro ufficio, la postazione di lavoro viene trasferita contestualmente al dipendente stesso, senza che si renda necessaria la preventiva autorizzazione da parte del Direttore della struttura di provenienza.

Rischi connessi a un cattivo utilizzo del PC assegnato

- disservizi
- costi straordinari di manutenzione
- minacce alla sicurezza

L’accesso all’elaboratore è protetto da password che è personale e deve essere custoDipartimento Innovazione Tecnologicaa dall’assegnatario con la massima diligenza e non resa nota a terzi.

Non è consentito installare sul personal computer in dotazione, software diversi da quanto previsto dall'Amministrazione, salvo preventiva e formale autorizzazione del Referente informatico di struttura, sentito il Direttore della struttura stessa e il responsabile dei Sistemi Informatici Distribuiti del Dipartimento Innovazione Tecnologica.

In caso di necessità di acquisto o installazione di software applicativi e/o procedure pertinenti esclusivamente ad alcune aree, deve essere comunque richiesto parere al Direttore del Dipartimento Innovazione Tecnologica, o suo delegato, per verificare che rimanga garantita la compatibilità funzionale e tecnica, nonché il mantenimento dell'efficienza operativa dei sistemi e delle reti.

Rischi connessi

- danneggiamenti del sistema per incompatibilità con il software esistente

Non è consentito all'utente modificare le caratteristiche hardware e software del proprio PC, salvo autorizzazione preventiva e formalmente espressa del referente Informatico di struttura, sentito il Direttore della struttura stessa e il responsabile dei Sistemi Informatici Distribuiti del Dipartimento Innovazione Tecnologica.

Salvo diverse indicazioni dei responsabili del Dipartimento Innovazione Tecnologica, il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

Prima di lasciare la postazione di lavoro è sempre necessario bloccare il computer mediante la contemporanea pressione dei tasti “ctrl+alt+canc” e la successiva pressione del tasto «Invio».

Rischi se si lascia incustodito un elaboratore connesso alla rete

- utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l’indebito uso

Non è consentito modificare i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi, salvo autorizzazione esplicita del Direttore del Dipartimento Innovazione Tecnologica o suo delegato.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d’ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito utilizzare le credenziali di terzi per accedere al computer, ai software e ai servizi internet.

I Responsabili del Dipartimento Innovazione Tecnologica o, in alternativa, il Referente Informatico della Struttura, sentito il Direttore della Struttura stessa, possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere contrari alle regole dettate in questa circolare.

Pulire periodicamente (almeno ogni sei mesi) gli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un’archiviazione ridondante.

È cura dell’utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

Le Utenze di accesso al computer e ai servizi internet sono attribuite secondo le modalità definite dal Dipartimento Innovazione Tecnologica. L'utente procederà alla modifica della password al primo utilizzo e, successivamente, almeno ogni sei mesi. Nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi (punto 5 del disciplinare tecnico allegato al Codice della privacy, D.Lgs. n. 196/2003 es.m.i.)

I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico allegato al Codice della privacy, D.Lgs. n. 196/2003 es.m.i.) devono essere custoditi in archivi chiusi a chiave.

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico allegato al Codice della privacy, D.Lgs. n. 196/2003 es.m.i.).

Rischi

- Una persona esperta potrebbe recuperare i dati memorizzati anche dopo la loro cancellazione

Il dipendente è inoltre responsabile del PC portatile, se assegnatogli, e deve custodirlo con diligenza sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.

Se utilizzati all’interno della rete LAN di Roma Capitale, ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete. All’utente assegnatario di PC portatile, è richiesta particolare attenzione nella rimozione di eventuali file elaborati prima della riconsegna dello stesso.

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo. Se il software antivirus rileva la presenza di un virus…

a) sospendere ogni elaborazione in corso
b) segnalare l'accaduto al Referente Informatico della Struttura che provvederà ad inoltrare tempestivamente la segnalazione ai presidi tecnici presso il Dipartimento Innovazione Tecnologica, per le azioni necessarie al superamento della minaccia o, in caso peggiore, del danneggiamento.

Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al Referente Informatico.

Responsabilità del Direttore di struttura

- Verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

Compiti del Referente Informatico di struttura

- aggiornare il database del parco macchine della struttura (compreso il caso di acquisizione di una o più apparecchiature per assegnazione di personale proveniente da altro ufficio).

Tutele connesse all'osservanza delle indicazioni del presente Manuale

- il diritto alla riservatezza ed alla dignità (Statuto dei lavoratori e D.Lgs. 196/03 es.m.i.)

La mancata osservanza delle indicazioni del presente Manuale o uso scorretto delle postazioni di lavoro

può costituire

- contravvenzione ai doveri di diligenza e fedeltà (artt. 2104 e 2105 cc, art. 23 CCNL)

può avviare

- provvedimenti disciplinari, se previsti, nonché le azioni civili e penali consentite