

Regolamento all'uso degli strumenti informatici.

 ca-campania.com/regolamento-alluso-degli-strumenti-informatici/

vincenzo de prisco

destinatari : RPCT, Titolare, DPO, RTD,
Amministratore di Sistema, Apicali, RSU.

Questo regolamento deve essere adottato per l'uso di strumenti informatici, qualora l'ente abbia già adottato uno strumento simile deve comunicarmelo all'indirizzo PEC ca@infopec.net , inoltre si ricorda che deve essere condiviso con la componente sindacale.



Premesse importanti :

- questo regolamento attua le politiche di sicurezza, anche organizzative della propria organizzazione
- questo regolamento contempla la norma contenuta nell'articolo 12 commi 3 e 3 bis del D.Lgs 82/05, quindi si applica ai device anche non di proprietà od in possesso dell'Ente , ma di proprietà od in possesso del dipendente dell'Ente , c.d. BYOD
- questo regolamento coniuga ed attua le seguenti norme , la L. 300/70 art 4 c 1, il D.Lgs 196/03, Il reg. 2016/279 per quanto riguarda l'utilizzo degli strumenti informatici ed è vincolante tra le parti una volta approvato
- questo regolamento deve essere diffuso ai dipendenti e valgono ai sensi degli articoli 2104 e 2105 del codice civile
- ai fini di questo regolamento per strumenti informatici si intendono strumentazioni hardware, software , locali, dipartimentali, cloud od in altra tecnologia

Parte 1 . Regole generali

1. **non è consentito installare autonomamente programmi provenienti dall'esterno** salvo previa autorizzazione esplicita dell'amministratore di sistema, in quanto sussiste il grave pericolo di portare virus e di creare rischi seri per la sicurezza informatica.
2. **non è consentito l'uso di programmi diversi da quelli distribuiti ed installati** ufficialmente dal responsabile dei sistemi informatici.
L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.

3. **non è consentito all'utente modificare le caratteristiche impostate sul proprio PC**, salvo previa autorizzazione esplicita dell'amministratore di sistema. Il personal computer, inoltre, deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.
4. **non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione**, comunicazione o altro (come ad esempio masterizzatori, modem, ecc...), se non con l'autorizzazione espressa dell'amministratore di sistema. A tal proposito sarebbe altamente consigliato per l'azienda impedire la possibilità per i dipendenti /incaricati di poter salvare i dati e portarli all'esterno bloccando, per esempio, gli accessi alle usb o adottando procedure analoghe.
5. **l'accesso agli strumenti è protetto da password**; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema. A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza. Certamente non con post-it attaccati al PC. A tal proposito è bene responsabilizzare i dipendenti sulle conseguenze di detto comportamento "apparentemente innocuo" e sulle responsabilità che ne derivano.

I controlli effettuati dal datore di lavoro sugli strumenti informatici non sono lesivi della riservatezza se non finalizzati al controllo a distanza in forza dell'articolo 4 della L. 300/70 – cassazione 10955/2015 – CEDU 2017

Si allega e si diffonde assieme alle regole qui scritte il doc. web n. 1387522 intitolato **le linee guida del Garante per posta elettronica e internet**

Inoltre al fine di diffondere la cultura della protezione dei dati l'Ente attraverso i social, newsletter e lezioni frontali promuove il seguente programma formativo :

Obiettivi della formazione, diffondere i nuovi standard di consapevolezza, vedi il post che segue sulle LLGG AGID SICUREZZA INFORMATICA

| LL.GG. AGID Sicurezza Cibernetica. Il danno erariale. La circolare 2/2017 AGID.