A cura della Commissione Informatica e Qualità

MODELLO DI REGOLAMENTO
PER L'UTILIZZO DEI SISTEMI INFORMATICI

AUTORE DEL DOCUMENTO

A cura di

Documento originale redatto da:
Luca RALLI
Maria Cristina DI BARTOLOMEO

Revisionato da:
Commissione Informatica e Qualità
dell'Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma

INDICE

Introduzione - Scopo

Il presente documento ha lo scopo di descrivere le principali regole da seguire durante l'attività lavorativa per quanto riguarda l'utilizzo dei sistemi informatici messi a disposizione dall'organizzazione (impresa/studio professionale/ente etc) che lo adotta ed entra in vigore al momento della sua approvazione indicata nell'ultimo paragrafo.

Le regole relative all'utilizzo dei sistemi informatici possono essere così riassunte:

PRIVACY

PROTEZIONE

PRUDENZA

Applicabilità

Il presente documento si applica nell'ambito del mantenimento in funzione dei sistemi informatici aziendali utilizzati e della protezione dei dati aziendali di lavorazione. Devono attenersi alla presente istruzione tutti i lavoratori, che a diverso titolo sono autorizzati ad accedere alle attività dell'azienda.

Per lavoratori si intendono:

- gli amministratori;
- i dirigenti;
- i dipendenti ed i collaboratori;
- gli stagisti;
- il personale fornito da terze parti;
- i consulenti;
- i membri di organi aziendali etc.

Quanto espressamente previsto nelle note organizzative ad oggi in vigore si intende abrogato e sostituito dal presente documento.

Distribuzione

La presente istruzione viene distribuita a:

- Tutti gli uffici
- Tutti i collaboratori (compreso il personale fornito da terzi, consulenti tecnici, professionisti etc)
- Tutti i componenti degli organi sociali

È possibile consultare tale regolamento nell'area riservata del sito web ovvero chiederne copia al responsabile della privacy.

Responsabilità

La responsabilità relativa al processo di miglioramento continuo del presente regolamento è la seguente:

Pianificazione	Responsabile Sistema Gestione (SG)
Applicazione	Responsabile SG
Controllo	Responsabile SG, Direzione
Miglioramento	Direzione

Qualsiasi proposta di miglioramento può essere inviata alla Direzione.

Modalità operative

Le modalità operative descritte nei paragrafi successivi riepilogano i principali obblighi e divieti.

Dispositivi portatili

- Per dispositivo portatile si intende una qualsiasi strumentazione informatica trasportabile e comprende specificatamente anche dispositivi quali: notebook, tablet, telefoni, sistemi integrati (dispositivi *embedded*) etc.

- L'utente è responsabile del dispositivo portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

- Ai dispositivi portatili si applicano le regole di utilizzo indicate nel paragrafo relativo all'uso delle strumentazioni informatiche, con particolare attenzione alla rimozione di eventuali file elaborati sugli stessi prima della riconsegna.

- I dispositivi portatili utilizzati all'esterno (convegni, visite in azienda, ecc.), in caso di allontanamento, anche temporaneo, devono essere riposti in un luogo protetto.

- Il dispositivo portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari. Ogni utente è responsabile dell'integrità dei dati che conserva in locale e deve tenere in considerazione il fatto che i dati potrebbero essere persi o compromessi. A tale riguardo l'utente è tenuto a memorizzare in forma protetta (es. accesso al file con password), in modo adeguato al loro livello di criticità o riservatezza, eventuali informazioni riservate/segrete residenti sul PC ed effettuare, con cadenza quotidiana il salvataggio dei dati.

- Durante i viaggi il dispositivo portatile deve essere sempre trasportato come bagaglio a mano, e non va mai lasciato in vista nelle stanze di hotel, residence, alloggi, etc., bensì deve essere opportunamente richiuso in valigia o in un armadio, o in cassaforte in caso di assenza prolungata.

- I dispositivi portatili devono essere spenti prima di lasciare il luogo di lavoro ovvero in caso di allontanamento o assenza prolungata. E' obbligatorio impostare le funzioni di blocco automatico dello schermo o sospensione della sessione e sblocco con password.

- L'accesso alla rete aziendale tramite RAS (Remote Access Server) / Accesso Remoto deve avvenire in forma esclusivamente personale. È obbligatorio l'uso rigoroso della password. Al termine della sessione di lavoro è obbligatorio disconnettersi dal sistema RAS.

- Il dispositivo portatile deve essere periodicamente collegato alla rete interna per consentire l'aggiornamento del sistema operativo, dell'antivirus e degli altri software.

- Salvo esplicita e specifica autorizzazione è vietata la connessione a reti lan o wi-fi (pubbliche o private) diverse dalla rete aziendale. Le connessioni gratuite o aperte possono celare minacce alla sicurezza dei dati.

- In caso di furto, danneggiamento o smarrimento del dispositivo portatile si è tenuti ad effettuare immediata segnalazione al proprio Responsabile e provvedere a immediata denuncia nelle forme di rito alle autorità di Pubblica Sicurezza.

Gestione delle password

- La scelta della password è un elemento importantissimo per la sicurezza informatica di un ufficio, per questo motivo è necessario scegliere una password complessa che rispetti almeno i seguenti requisiti:
  - minimo 8 caratteri;
  - contenere almeno una maiuscola;
  - contenere almeno una minuscola;
  - contenere almeno un numero;
  - contenere almeno un carattere speciale tra quelli elencati: ! $? # = * + - . , ; :

- Le credenziali di accesso alla rete, sono attribuite per la prima volta dall'amministratore del sistema, il quale provvede alla comunicazione verbale o scritta all'incaricato che al primo accesso, sarà obbligato alla modifica della password con una di sua scelta, nel rispetto delle regole proposte al punto precedente. Inoltre è consigliabile entro il temine di 90 (novanta) giorni, che il sistema informatico provveda a far scadere la password e che l'incaricato provveda a generarne una nuova, per poter continuare ad accedere alla rete in tutta sicurezza.

- In caso di assenza prolungata di un incaricato, e qualora ci sia la necessità di aggiornare il computer o comunque di accedervi per una valida ragione, l'amministratore di sistema, in accordo con lo stesso, provvede a far scadere la password ed a generarne una nuova, permettendo l'accesso al computer in maniera temporanea, per il tempo necessario allo svolgimento dell'urgenza. Al temine dei lavori, l'amministratore di sistema, comunica la nuova password di accesso temporanea all'incaricato, che è obbligato dal sistema ad effettuare un "cambio password", garantendo nuovamente la segretezza della password.

- L'incaricato è tenuto a scollegarsi dal sistema (bloccando il PC) ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicato il dispositivo o nel caso ritenga di non essere in grado di presidiare l'accesso al medesimo. Lasciare un dispositivo incustodito connesso alla rete può

essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

- Non si deve rivelare o far digitare la password dal personale di assistenza tecnica. Non si deve rivelare mai la password al telefono né si deve inviarla via email o fax (nessuno è autorizzato a richiederla). Segnalare qualsiasi stranezza o anomalia al Responsabile.

Protezione antivirus

- Ogni personal computer o dispositivo analogo deve essere protetto da un antivirus aggiornato. E' obbligatorio comunicare al responsabile dei sistemi informatici eventuali necessità di rinnovo o situazioni che impediscono l'aggiornamento del software.

- Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico da parte di virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali, ecc.).

- Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso **senza spegnere il computer** e segnalare l'accaduto all'Amministratore di Sistema.

- Ogni dispositivo di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso sia rilevato un virus l'utente dovrà immediatamente sospendere ogni elaborazione in corso **senza spegnere il computer** e segnalare l'accaduto all' Amministratore di Sistema.

Uso della navigazione Internet

- II PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

- Per la navigazione è obbligatorio utilizzare i browser presenti sul pc, senza l'installazione di plugin aggiuntivi, e solo se l'antivirus è attivo ed aggiornato.

- E' proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

- Astenersi da operazioni di download / upload di files particolarmente pesanti programmandoli, ove possibile, in orari "non di punta".

- Non possono essere utilizzati modem o hardware privati per il collegamento alla rete.

- E' fatto divieto all'utente di eseguire download di software gratuito freeware o shareware prelevato da siti Internet, se non espressamente autorizzato dalla direzione.

- E' vietata la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati),di bacheche elettroniche e le registrazioni in guestbook anche utilizzando pseudonimi o nickname.

- È vietato il trasferimento di qualsiasi file o parti di esso, a qualunque titolo, attraverso programmi di chat o altri servizi.

- E' vietata la navigazione in siti non sicuri o segnalati come tali dal software antivirus. E' altresì vietata la navigazione nel deep web, dark web o altre reti analoghe.

- Evitare di far registrare le password dal Browser utilizzato per la navigazione.

- In caso di navigazione da un dispositivo diverso da quello aziendale utilizzare gli strumenti di eliminazione della cronologia o la navigazione anonima.

Uso della posta elettronica

- L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del Responsabile di funzione/unità organizzativa all'Amministratore di sistema.

- La casella di posta assegnata dall'Azienda all'utente è uno strumento di lavoro aziendale. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse (art. 615 comma 5 e segg. c.p.).

- L'accesso alla posta elettronica può essere effettuato da remoto utilizzando il sito webmail con protocollo HTTPS.

- Il software per l'accesso alla posta elettronica deve essere autorizzato e configurato dall'amministratore di sistema.

- Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli eliminandoli anche dal cestino.

- Nel caso di messaggi contenenti allegati sospetti (file con estensione es. .EXE, .CMD, .BAT, .SCR, .JAR, .PIF, .COM, .DLL, .MSC, .MSI, .HTA, .MSP, JS, .PS1, .PS2, REG, .LNK, .INF), anche se provenienti da mittenti conosciuti, non aprire assolutamente né il messaggio né l'allegato cancellandoli ed eliminandoli anche dal cestino.

- L'iscrizione a mailing list esterne è concessa solo per motivi professionali. Prima di iscriversi occorre verificare in anticipo se il sito è da considerarsi affidabile, attendendo all'uopo autorizzazione scritta da parte della direzione.

- La casella di posta deve essere mantenuta in ordine, cancellando periodicamente messaggi e documenti obsoleti o inutili dopo averlo convenuto con il Responsabile di funzione.

Uso della rete e di Internet

- L'accesso alla rete aziendale è protetto da password. Per eseguire il login devono essere inserite le credenziali assegnate (nome utente e password). Le credenziali devono essere conservate con cura e non devono essere divulgate.

- La rete internet ed i servizi aziendali sono risorse messe a disposizione esclusivamente come strumenti di lavoro e fonte di informazioni per finalità lavorative di documentazione, ricerca e studio.

- La navigazione su taluni siti web può essere limitata dal responsabile dei sistemi.

- L'uso di social network deve essere preventivamente autorizzato e si intende sempre limitato a fini lavorativi coerenti con la propria posizione.

- L'utilizzo delle cartelle di rete o di Internet per scopi extra lavorativi è vietato. E' fatto divieto di utilizzare software o servizi non inerenti l'attività lavorativa ed è vietata la partecipazione a forum non legati alla prestazione lavorativa, l'utilizzo di chat line, bacheche elettroniche etc.

- Si possono effettuare copie di dati su supporti rimovibili (es. dischetti CD, DVD, chiavi usb) solo se finalizzati a scopi lavorativi. Al termine del trattamento sarà cura del dipendente distruggere o rendere inutilizzabili i dati salvati sui supporti rimovibili eventualmente utilizzati.

- Ognuno si deve impegnare ad evitare un'archiviazione ridondante dei dati che non consenta in modo chiaro ed inequivocabile, l'identificazione dello stato di revisione di un documento.

- Gli spazi di archiviazione e la velocità di trasmissione dati sono risorse limitate. E' obbligatorio contenere al minimo la dimensione dei files ponendo quotidiana attenzione al proprio lavoro.

- Sugli spazi condivisi di archiviazione saranno svolte regolari attività di verifica e/o backup da parte dei responsabili appositamente incaricati, i quali potranno, previa autorizzazione della direzione, procedere alla rimozione di ogni file o applicazione che riterranno pericolosa per la sicurezza o non inerente l'attività lavorativa.

- E' vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione da parte del responsabile sistemista aziendale.

- E' vietato monitorare ciò che transita in rete.

- E' vietata l'installazione non autorizzata di dispositivi che sfruttino il sistema di comunicazione per l'accesso a banche dati esterne o interne all'azienda.

Uso delle strumentazioni informatiche

- Per strumentazioni informatiche si intendono tutti i dispositivi elettronici atti a elaborare o immagazzinare informazioni quali ad esempio: telefoni, cellulari, centralini, personal computer, tablet, server, nas, pendrive, router, switch, access point etc. Nel concetto di strumentazioni informatiche rientrano anche i relativi software, compresi quelli fruibili in modalità SAAS (software as a service es. centralini telefonici virtuali)ed i firmware.

- Le strumentazioni informatiche sono strumenti di lavoro. Ognuno è responsabile dell'utilizzo delle strumentazioni informatiche che devono essere tenute con estrema cura per evitare malfunzionamenti.

- Ogni utilizzo delle strumentazioni informatiche non coerente all'attività lavorativa di destinazione può contribuire a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza pertanto è vietato modificare le caratteristiche hardware e software impostate sui dispositivi e servizi che di volta in volta si utilizzeranno, anche in collegamento remoto, salvo autorizzazione esplicita da parte della Direzione ovvero del responsabile dei sistemi informatici.

- E' vietato l'uso di supporti di archiviazione removibili (chiavette USB, hard disk, CD-Rom, ecc.) o spazio web personale, per la memorizzazione di file di qualsiasi estensione contenenti dati relativi a pratiche in gestione se non per usi inerenti all'attività lavorativa o a seguito di autorizzazione scritta da parte del Responsabile.

- Le gestioni locali dei dati dovranno scomparire per essere sostituite da gestioni centralizzate su server.

- Non è consentita l'installazione di plugin a software esistenti (es. plugin dei browser)

- Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21/05/2004.

- Gli operatori responsabili del Sistema Informativo possono, in qualunque momento, procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza, sia sui PC di ogni singolo utente che sulle unità di rete.

- In presenza di ospiti farli attendere in luoghi in cui non siano presenti informazioni riservate o dati personali e, come sempre, se è necessario allontanarsi dalla scrivania in presenza di ospiti riporre i documenti ed attivare il salvaschermo (con password) del proprio PC.

- Nel caso di utilizzazione di stampanti o scanner, verificare che gli stessi non lascino copie locali dei documenti gestiti (salvataggio automatico).

- La cancellazione di un file, anche dal "cestino", non ne assicura la eliminazione definitiva dal PC.

Normativa di riferimento e sanzioni

Osservanza delle disposizioni in fatto di privacy:

- È obbligatorio attenersi alle disposizioni in materia di privacy e di misure minime di sicurezza contenute nel decreto legislativo n. 196 del 30 giugno 2003 e successive modificazioni e in questo si rimanda a quanto riportato sulla personale nomina a incaricato (rif. http://www.garanteprivacy.it)

- E' vietata la diffusione a terzi delle informazioni relative ai sistemi informatici aziendali, regolamenti interni, informazioni tecniche ed accadimenti aziendali in genere.

Non osservanza della normativa aziendale:

- Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari, ivi compreso il licenziamento, nonché con le azioni civili e penali previste dalle leggi.

Legge 22 aprile 1941, n. 633, articoli 171, 171 bis e 171 ter.
Legge 248 del 2000 Allegato B al D. Lgs. 196/03 Disciplinare tecnico in materia di misure minime di sicurezza.
Codice Penale:
- Art.594: Ingiuria
- Art.595: Diffamazione
- Art.600 ter: Pornografia minorile
- Art.600 quarter: Detenzione di materiale pornografia

- Art.600 quater bis: Pornografia virtuale
- Art.600 sexies: Circostanze aggravanti ed attenuanti
- Art.600 septies: Confisca e pene accessorie
- Art.615 ter: Accesso abusivo ad un sistema informatico o telematico
- Art.615 quarter: Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Art.615 quinques: Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- Art.617 quarter: Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Art.617 quinquies: Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.
- Art.617 sexies: Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche
- Art.635 bis: Danneggiamento di informazioni, dati e programmi informatici
- Art. 635-quater Danneggiamento di sistemi informatici o telematici
- Art.640: Truffa
- Art.640 ter: Frode informatica

Aggiornamenti del regolamento

Il presente documento è stato oggetto delle seguenti modifiche:

___/___/_____ (Prima emissione)

***

Approvazioni:

Redatto: _____

Verificato da: _____

Approvato da: _____

***

CHECK-LIST
dei sistemi informatici dello studio
2016

AUTORE DEL DOCUMENTO

A cura di

Documento originale redatto da:
Luca RALLI
Maria Cristina DI BARTOLOMEO

Revisionato da:
Commissione Informatica e Qualità
dell'Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma

Il controllo periodico della infrastruttura I.T. è un compito che dobbiamo delegare ai tecnici… …ma NOI sappiamo di cosa c'è bisogno?

Proviamo a compilare la check list dei sistemi informatici del nostro studio.

CHECK-LIST I.T.

1. E' stato installato un firewall?
2. Chi si occupa dell'assistenza tecnica in caso di malfunzionamento?
3. Esiste una linea elettrica protetta? Un gruppo di continuità unico per router, firewall, switch, telefoni, server, pc…?
4. Il WI-FI è protetto da una password forte?
5. Il server è chiuso a chiave in un armadio rack o simile?
6. L'armadio rack / locale server è ventilato?
7. La rete locale è stata certificata?
8. La rete locale ha una velocità in linea con quanto dichiarato dall'installatore (e' stato eseguito un test)?
9. Le connessioni LAN sono accessibili solo dal personale?
10. Esiste un sistema di backup automatico?
11. Si dispone di un NAS?
12. E' stata pianificata una verifica periodica del backup?
13. E' stato redatto il DVR considerando anche i rischi I.T.?
14. Esiste una copia degli archivi esterna allo studio?
15. Il personale è adeguatamente formato (es. su criptolocker ed uso della mail, copie di backup etc.)?
16. I pc dispongono di almeno due account amministratore?
17. I software installati sui pc sono in regola con le licenze?
18. Il sito WEB è a norma con le disposizioni sulla privacy?
19. Il sito WEB è localizzato presso un ISP?
20. Il sito WEB è reattivo (responsive)?

21. Il sito web è SEO? (ottimizzato per i motori di ricerca)
22. L'antivirus è una versione professionale?
23. L'antivirus è installato su tutti i dispositivi?
24. Sui pc c'e' una password forte?

IN CASO DI GRAVE DISASTRO INFORMATICO:

25. … RIESCO A TORNARE OPERATIVO?
26. … IN QUANTO TEMPO?