REGOLAMENTO INTERNO PER LA SICUREZZA INFORMATICA E L'UTILIZZO DELLA RETE E DELLE POSTAZIONI DI INFORMATICA

Sommario

Articolo 1. Finalità

1. Premesso che l'utilizzo delle risorse informatiche e telematiche Aziendali deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che, normalmente, sono basilari in un rapporto di lavoro, l'ARPAM adotta il presente regolamento per la sicurezza informatica, al fine di contribuire alla massima diffusione della cultura sulla sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.
2. L'ARPAM promuove ogni opportuna misura organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati e disciplina le modalità con cui effettuerà i relativi controlli.
3. Il presente Regolamento, viene incontro, quindi, alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e contiene informazioni utili per garantire la sicurezza informatica di tutta l'ARPAM.

Articolo 2. Oggetto ed ambito di applicazione

1. Il presente regolamento disciplina le corrette modalità di utilizzo della rete informatica dell'ARPAM, nonché le corrette modalità di utilizzo delle postazioni di informatica individuale, in conformità e nel rispetto di quanto stabilito dal D.Lgs n. 196/2003 s.m.i., dal Regolamento ARPAM in materia di privacy, dal Documento Programmatico sulla Sicurezza ARPAM, dalle normative di settore, nonché dalle norme che disciplinano e tutelano il lavoro alle dipendenze della Pubblica Amministrazione. Il regolamento si ispira, altresì, alle "Linee giuda per la definizione di un piano di sicurezza dei sistemi informativi automatizzati nella Pubblica Amministrazione" dell'AIPA.
2. Ai fini dell'applicazione del presente Regolamento, si intende per "rete informatica", l'insieme delle risorse infrastrutturali (hardware/software e apparati elettronici collegati alla rete) e del patrimonio informativo digitale (banche dati in formato digitale e, in generale, tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati).
3. Il presente Regolamento si applica a tutti gli utenti interni ed esterni che sono autorizzati ad accedere alla rete ARPAM. In particolare, per "utenti interni", si intendono tutti i Dirigenti, i dipendenti ed i collaboratori occasionali, mentre, per "utenti esterni", si intendono le ditte fornitrici di hardware e software, che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, professionisti esterni, enti, etc., che siano autorizzati da espressa lettera di nomina a "Responsabile esterno al trattamento dati" all'accesso a specifiche banche dati con le modalità in esse stabilite.
4. E' vietato il controllo riguardante l'utilizzo degli strumenti informatici aziendali utilizzati per l'espletamento di attività lavorativa in senso stretto, ad esclusione dei casi connessi ad esigenze produttive ed organizzative (ad esempio, per rilevare anomalie, per manutenzione o per la sicurezza sul lavoro).

Articolo 3. Principi generali – Diritti e responsabilità

1. L'ARPAM promuove l'utilizzo della Rete Informatica, di Internet Intranet e della Posta Elettronica, quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali.
2. Le comunicazioni tra l'Amministrazione ed i propri dipendenti avvengono, di preferenza, tramite posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.
3. Ogni utente è responsabile civilmente e penalmente del corretto uso delle Risorse informatiche, dei Servizi/programmi ai quali ha accesso e dei propri dati, del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.
4. Sono vietati comportamenti che possono creare un danno, anche di immagine, all'ARPAM. Nell'utilizzo degli strumenti l'utente si attiene ai principi e ai doveri stabiliti nel "Codice di comportamento" in vigore.

Articolo 4. Utilizzo del Personal Computer – Hardware e periferiche

1. Il Personal Computer affidato all'utente è uno strumento di lavoro. Ognuno è personalmente responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
2. Non è consentito all'utente di modificare le caratteristiche hardware e software impostate sul proprio PC, senza la preventiva autorizzazione del Dirigente Responsabile di concerto con il Responsabile Informatico.
3. Il Personal Computer e le Stampanti debbono essere spenti al termine di ogni giornata lavorativa prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio, salvo quelli/e in uso ai laboratori e quando sussistano esigenze particolari e motivate, autorizzate dal Direttore del Dipartimento/Direttore Amministrativo.
4. Le informazioni archiviate informaticamente devono essere esclusivamente quelle necessarie all'attività lavorativa, tenuto conto di quanto prevede la legge, nonché delle rispettive competenze ed attribuzioni professionali.
5. Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili (.tmp). Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.
6. La tutela della gestione locale di dati su stazioni di lavoro personali – personal computer che gestiscono localmente documenti e/o dati - è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo. E' comunque vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili, in accordo con quanto dettato nel Documento Programmatico sulla Sicurezza dell'ARPAM.

7. Non è consentita l'installazione di programmi diversi da quelli autorizzati ed utilizzati per fini istituzionali e di lavoro.
8. Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n. 128 del 21.05.2004, di conversione in legge del D.L. 22 marzo 2004, n. 72. E' vietato cancellare, copiare o asportare programmi software per scopi personali e/o cedere programmi e altro materiale informatico, se non nella forma e per gli scopi di servizio per i quali sono stati assegnati.
9. Non è consentito installare componenti hardware non compatibili con l'attività istituzionale e componenti hardware non autorizzati non di proprietà dell'ARPAM, né rimuovere, danneggiare o asportare componenti hardware.
10. I Sistemisti e i Tecnici informatici potranno in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.
11. I Sistemisti e i Tecnici informatici e/o incaricati alla gestione e alla manutenzione dei componenti del sistema informativo possono in qualsiasi momento, accedere al personal computer (anche con strumenti di supporto, assistenza e diagnostica remota) per manutenzione preventiva e correttiva.
12. L'eventuale malfunzionamento o danneggiamento del personal computer dovrà essere tempestivamente comunicato al Direttore di Dipartimento e all'ufficio informatico.
13. Ogni utente che dovrà per qualsiasi motivo lasciare incustodita la propria postazione di lavoro sarà tenuto a chiudere tutte le applicazioni in modo corretto e/o bloccare l'accesso o spegnere fisicamente il computer.

Articolo 5. Utilizzo della Rete Intranet

1. L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale (username e password).
2. E' fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati o per scopi non connessi o difformi con l'espletamento dell'attività lavorativa istituzionale.
3. E' vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione.
4. E' vietato condividere cartelle in rete (sia dotate di password, sia sprovviste di password) se non mediante formale autorizzazione scritta del rispettivo Responsabile della struttura al Responsabile/Referente Informatico.
5. E' vietato monitorare ciò che transita in rete, nonché utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber), software di decodifica password (cracker) e, più in generale, software rivolti alla violazione ella sicurezza del sistema e della privacy.
6. E' vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'azienda.
7. E' vietato inserire nelle cartelle di rete (sia le proprie che quelle comuni) file molto pesanti, perché potrebbero riempire l'hard disk del server. L'inserimento di tali file può avvenire previa autorizzazione del rispettivo Responsabile della struttura, sentito il Responsabile/Referente Informatico.

8. E’ vietato conseguire l’accesso non autorizzato a risorse di rete interne o a risorse di rete esterne, tramite la stessa Rete dell’ARPAM.
9. E’ vietato agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l’utilizzabilità e le prestazioni per altri utenti.

Articolo 6. Gestione delle password

1. L’account è costituito da un username e da una password.
2. Le password d’ingresso alla rete, di accesso ai programmi informatici e ad internet vanno predisposte, custodite e modificate secondo le modalità previste nel Documento Programmatico sulla Sicurezza dell’ARPAM.
3. La password non deve contenere riferimenti agevolmente riconducibili all’utente.
4. L'utente è tenuto a conservare nella massima segretezza la propria password di accesso alla rete ed ai sistemi, nonché qualsiasi altra informazione legata al processo di autenticazione.
5. La password deve essere immediatamente sostituita in caso si sospetti che la stessa abbia perso la segretezza, dandone comunicazione al Responsabile/Referente informatico, nelle modalità previste nel Documento Programmatico sulla Sicurezza dell’ARPAM.
6. Non è consentita l'attivazione della password d'accensione (bios), senza la preventiva autorizzazione del Responsabile/Referente Informatico, nominato presso ciascuna sede dell’ARPAM.
7. In caso di cessazione del rapporto di lavoro, l’account individuale dell’utente verrà immediatamente dismesso.
8. E’ compito dell’Ufficio informatico e dei Responsabili/Referenti informatici di aggiornare tempestivamente le variazioni del personale sulla rete.

Articolo 7. Utilizzo di PC portatili

1. L'utente è responsabile del PC portatile assegnatogli dall'ARPAM e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
3. I PC portatili utilizzati all'esterno (convegni, visite in azienda, etc.), in caso di allontanamento, devono essere custoditi in luogo protetto.
4. II PC portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.
5. L’utente dovrà collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.
6. E’ vietato utilizzare abbonamenti Internet privati per collegamenti alla rete se non autorizzati dal Responsabile della struttura.

Articolo 8. Uso della posta elettronica

1. A ogni dipendete è assegnata una casella di posta elettronica. Eventuali particolari abilitazioni devono essere precedute da regolare richiesta del rispettivo Responsabile di struttura al Responsabile Informatico.

2. La casella di posta, assegnata dall'ARPAM, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. E' fatto divieto di utilizzare la casella di posta elettronica per fini non espressamente autorizzati o per scopi non connessi con l'espletamento dell'attività lavorativa istituzionale.
3. E' fatto divieto di comunicare il proprio indirizzo di posta elettronica su siti web sospetti e/o mailing list non direttamente collegate alla propria attività lavorativa istituzionale.
4. Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, l'utente dovrà cancellare i messaggi senza aprirli.
5. Nel caso di messaggi provenienti da mittenti conosciuti, ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti ed i messaggi dovranno essere cancellati.
6. In entrambi i casi previsti ai punti 4 e 5 del presente articolo, è obbligatorio evitare di inviare ad altri utenti il messaggio sospetto.
7. L'utente deve adottare comportamenti finalizzati ad evitare che la diffusione incontrollata di messaggi a diffusione capillare e moltiplicata ("Catene di Sant'Antonio") limiti l'efficienza del sistema di posta.
8. L'utente deve utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rar *.jpg).
9. Nel caso in cui si debba inviare un documento all'esterno dell'ARPAM, è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf).
10. L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile e non oneroso.
11. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e, soprattutto, allegati ingombranti; i messaggi di posta vecchi devono essere archiviati in supporti per non appesantire l'efficienza del PC.
12. Per la trasmissione di file via elettronica, bisogna far attenzione alla dimensione degli allegati che non devono mai superare i 5 MB.
13. E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Articolo 9. Uso della rete Internet e dei relativi servizi

1. Tutti i PC sono abilitati alla navigazione in Internet, solo perché costituisce uno strumento per finalità aziendali necessarie allo svolgimento della propria attività lavorativa.
2. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa (es. uso per motivi personali, accesso a siti inappropriati, etc).
3. Non possono essere utilizzati modem privati per il collegamento alla rete.
4. E' fatto divieto all'utente lo scarico di software, sia freeware (gratuito) che shareware, prelevato da siti Internet, se non espressamente autorizzato dal Responsabile della struttura. Il software scaricato può contenere virus o essere incompatibile con programmi già installati.
5. E' fatto divieto all'utente lo scarico di files, audio e video, prelevati dai siti Internet, se non espressamente autorizzati dal Responsabile della struttura. I files scaricati possono contenere virus.

6. E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books, anche utilizzando pseudonimi (nicknames).
7. E' vietato utilizzare programmi per la condivisione e lo scambio di file in modalità "peer to peer" (Napster, Emule, Winmx, E-Donkey, ect.), nonché accedere a flussi in streaming audio/video da Internet per scopi non istituzionali (ad esempio, ascoltare la radio, guardare video o filmati).

Articolo 10. Protezione Antivirus

1. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus dialer spamspyware o di ogni altro software aggressivo. In particolare, ogni utente non deve aprire mail o relativi allegati sospetti, non deve navigare su siti non professionali, non deve mai scaricare dialers di connessione da siti che propongono di farlo, rispondendo sempre "NO" a questo tipo di finestre.
2. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale tramite l'icona blu a destra dello schermo.
3. 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, spegnere il computer e segnalare l'accaduto al Responsabile/Referente Informatico.
4. Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo.
5. Modalità e funzionamento del sistema antivirus ARPAM sono previste nel Documento Programmatico sulla Sicurezza dell'ARPAM.

Articolo 11. Utilizzo delle stampanti e dei materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è consentito esclusivamente ai compiti di natura strettamente istituzionali.
2. Al fine di evitare in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi, il dipendete, deve adottare, nella propria attività lavorativa, i seguenti accorgimenti:
   - stampare e-mail e documenti solo quando strettamente necessario;
   - utilizzare quanto più possibile le fotocopiatrici collegate in rete per la stampa di documenti e altro per ridurre i consumi energetici e le cartucce d'inchiostro delle stampanti;
   - utilizzare, quando è possibile, le stampe fronte-retro;
   - cercare di ottimizzare lo spazio all'interno di una pagina;
   - procedere quanto più possibile alla scannerizzazione dei documenti e all'archiviazione informatica piuttosto che cartacea;
   - quando è possibile, trasmettere testi, documenti, relazioni, ecc. attraverso e-mail invece di copie cartacee;
   - modificare la risoluzione di stampa, utilizzando la qualità di stampa "bozza", per ridurre il consumo di toner;
   - evitare di utilizzare, quando possibile, la stampa a colori.

- riutilizzare la carta già stampata su un solo lato per gli appunti o per stampe di prova.

Articolo 12. Controlli, responsabilità e sanzioni

1. Gli utenti sono obbligati a conformarsi alle disposizioni del presente regolamento, nonché a quanto dettato nel Documento Programmatico sulla Sicurezza.
3. L'ARPAM si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici, della posta elettronica, di internet, delle stampanti e materiali di consumo, nel rispetto delle normative vigenti e del presente regolamento.
4. Per esigenze organizzative, produttive e di sicurezza l'ARPAM può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, servizi o gruppi di utenti.
5. Qualora durante un controllo generalizzato vengano rilevate anomalie nell'utilizzo degli strumenti informatici, l'ARPAM procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente regolamento e alla normativa vigente, e si riserva la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.
6. Il mancato rispetto o la violazione da parte degli utenti dei principi e delle norme contenute nel presente regolamento comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia, previo espletamento del procedimento disciplinare, nonché le azioni civili e penali previste dalle leggi.

Articolo 13. Entrata in vigore e pubblicità

1. Il presente regolamento entrerà in vigore tramite approvazione con apposito Decreto del Direttore Generale.
2. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
3. Copia del regolamento sarà disponibile per ciascun dipendente e collaboratore dell'ARPAM, a prescindere dal rapporto contrattuale con la stessa intrattenuto, tramite pubblicazione sul sito Intranet aziendale.