REGOLAMENTO ASSOCIAZIONISTICO INTERNO PER LA SICUREZZA INFORMATICA, L'UTILIZZO DEGLI STRUMENTI ELETTRONICI, DI INTERNET E DELLA POSTA ELETTRONICA

Indice

Premessa

L'illecito utilizzo della strumentazione informatica associazionistico da parte dei soci, collaboratori e dipendenti, può generare in capo all'Associazione, una serie di responsabilità sia penali che civili creando problemi alla sicurezza e all'immagine dell'Associazione stessa.

Premesso che l'utilizzo delle risorse informatiche e telematiche associazionistici deve sempre ispirarsi al principio della diligenza, correttezza ed eticità, comportamenti che normalmente sono basilari in un rapporto di lavoro, O.I.P.E.S. ha adottato il presente Regolamento, promosso dall'Associazione stessa nella persona del legale rappresentante Mauro Testarella insieme all'Amministratore del Sistema Informatico incaricato Adina Pinzi, alla luce del "Piano programmatico Aziendale sulla sicurezza informatica", per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. Il Regolamento associazionistici di seguito riportato disciplina le condizioni per il corretto utilizzo degli strumenti informatici da parte dei soci e dei collaboratori e contiene informazioni utili per comprendere cosa può fare ogni socio e/o collaboratore per contribuire a garantire la sicurezza informatica di tutta l'Associazione.

Tale prescrizione si aggiunge e integra le norme già previste dal contratto di collaborazione nonché in riferimento al Provvedimento del Garante per la Protezione dei Dati Personali, relativo al "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei soci/collaboratori" (in seguito definito semplicemente "Provvedimento" per brevità) datato 1° Marzo 2007 e pubblicato sulla Gazzetta Ufficiale n. 58 del 10 Marzo 2007 e dal relativo Documento Programmatico sulla Sicurezza adottato da O.I.P.E.S. in data 01/01/2016

ART.1) OGGETTO E AMBITO DI APPLICAZIONE

Il presente Regolamento disciplina le modalità di utilizzo dei Personal Computer, dei PC portatili, la gestione delle password, l'utilizzo dei software, l'utilizzo della posta elettronica nonchè l'accesso e uso della rete internet e dei relativi servizi all'interno di O.I.P.E.S. Il presente Regolamento si applica a tutti i soci di O.I.P.E.S. nonchè a tutti i suoi collaboratori e dipendenti con i quali ha in corso un rapporto di lavoro o di collaborazione e adi eventuali stagisti.

ART.2) UTILIZZO DEL PERSONAL COMPUTER

2.1) Il Personal Computer affidato al socio/collaboratore/dipendente è uno strumento di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività associazionistica può contribuire a creare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza con conseguenti vulnerabilità all'intero sistema informativo associazionistico.

2.2) Non è consentito l'utilizzo di Personal Computer che non siano proprietà di O.I.P.E.S. Soci, dipendenti e collaboratori potranno utilizzare solo ed esclusivamente i Personal Computer messi a disposizione da O.I.P.E.S.

2.3) Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte di O.I.P.E.S.

2.4) Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte dell'Amministratore di Sistema dell' O.I.P.E.S.

2.5)L'accesso al Personal Computer è regolamentato ed ogni socio/collaboratore/dipendente è in possesso del proprio account composta da Username e Password che dovranno essere utilizzate ogni qual volta si accede al PC.

2.6) Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

2.7) E' fatto divieto di lasciare libero accesso al PC che dovrà essere sempre protetto da password.

2.8) Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa.

2.9) 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 ogni caso è preferibile effettuare sempre il back-up sul server.

2.10) Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Sistema Informativo Associazionistico.

2.11) Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della legge n. 128 del 21.05.2004.

2.12) L'Amministratore di Sistema può in qualunque momento "controllare", anche durante operazioni di manutenzione e assistenza, e procedere alla rimozione di ogni file o applicazione soprattutto se ritenute essere pericolose per la

Sicurezza sia sui PC degli incaricati sia sulle unità di rete. Pertanto non si risponde di eventuali files "privati" mancanti.

ART.3) UTILIZZO DELLA RETE

3.1) L'accesso della rete aziendale potrebbe essere protetto da password; per l'accesso deve essere utilizzato esclusivamente il proprio profilo personale regolamentato da Username e Password.

2

3.2) E' fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati (a titolo esemplificativo ma non esaustivo vengono fatti i seg.ti esempi: chat, videochat, audiochat, P2P, streaming audio, streaming video, ecc).

3.3) E' vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Responsabile Sistemista Associazionistico.

3.4) E' vietato condividere cartelle in rete sia dotate di password, sia sprovviste di password se non dietro esplicita e formale autorizzazione dell'Amministratore di Sistema Associazionistico.

3.5) E' vietato monitorare ciò che transita in rete.

3.6) 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'associazione.

ART.4) USERNAME (NOME UTENTE)

4.1) Non permettere ad alcuno l'utilizzo del proprio identificativo personale. Come proprietario, ognuno è responsabile per qualsiasi attività svolta attraverso di esso. Se si sospetta che qualcuno stia utilizzando o abbia utilizzato il proprio identificativo personale, informare tempestivamente la Direzione per poter prendere le contromisure del caso.

4.2) Non tentare di autenticarsi su qualsiasi sistema utilizzando l'identificativo personale di altri.

ART.5)GESTIONE DELLE PASSWORD

5.1) Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dall'Amministratore di Sistema. Al riguardo è individuato un modulo di "Concessione/Revoca/Modifica abilitazioni applicative" che i responsabili dei trattamenti utilizzeranno per le comunicazioni del caso all'Amministratore di Sistema.

5.2) L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete e ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.

5.3) L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un elaboratore 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.

5.4) Le password devono essere formate da almeno 8 caratteri alfanumerici.

5.5) Le password non devono essere rappresentate da nomi propri, di cose, date o serie di numeri.

5.6) Le password non devono essere facilmente riconducibili alla persona (utente), quindi utilizzando, ad esempio, i nomi dei figli, degli animali domestici, l'anno di nascita.

5.7) Le password non devono essere incluse in nessun sistema automatico di logon o macro applicativa.

5.8) La password deve essere immediatamente sostituita, dandone comunicazione all'Amministratore di Sistema, nel caso si sospetti che la stessa abbia perso la segretezza. In ogni caso deve essere sostituita ogni sei mesi, così come previsto dal Disciplinare Tecnico in materia di misure minime di sicurezza

ART.6) UTILIZZO PC PORTATILI

6.1) L'utente è responsabile del PC portatile assegnatogli da O.I.P.E.S. e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

6.2) Non è consentito l'utilizzo di PC portatili che non siano proprietà di O.I.P.E.S..: soci, dipendenti e collaboratori potranno utilizzare solo ed esclusivamente i PC portatili messi a disposizione da O.I.P.E.S. in Sede.

Nei casi particolari in cui O.IP.E.S. autorizzi soci , dipendenti e collaboratori ad utilizzare il proprio PC portatile, non potranno essere trattenuti sugli stessi file associazionistici. Ad ogni modo anche in questo caso valgono tutte le regole previste dal presente Regolamento.

6.3) 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.

6.4) I PC portatili utilizzati all'esterno (convegni, visite in Sede), in caso di allontanamento, devono essere custoditi in un luogo protetto.

6.5) Il PC portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo file strettamente necessari.

6.6) Nel caso di accesso alla rete associazionistica tramite RAS (Remote Access Server)/Accesso Remoto: utilizzare l'accesso in forma esclusivamente personale e utilizzare la password in modo rigoroso.

6.7) Disconnetersi dal sistema RAS al termine della sessione di lavoro.
6.8) Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus, qualora quest'ultimo sia previsto.
6.9) Non utilizzare abbonamenti Internet privati per collegamenti alla rete.

ART.7) USO DELLA POSTA ELETTRONICA (modalità di connessione alla rete Internet I)
7.1) L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del responsabile di funzione/unità organizzativa all'Amministratore di Sistema.
7.2) La casella di posta assegnata dall'Associazione è uno strumento di lavoro.
Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse (art. 615-quinquies e segg. c.p.). A tal fine O.I.P.E.S. informa sin da ora i propri soci, dipendenti e collaboratori dell'eventualità di dover controllare la casella in loro uso, pur sempre e solo per motivi di ordine associazionistico e nel massimo rispetto della legge 196/2003.
7.3) Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.
7.4) 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.
7.5) Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
7.6) Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (per esempio: *.zip *.tar *.jpg).
7.7) Nel caso in cui si debba inviare un documento all'esterno dell'Azienda è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf).
Tale software specifico è fornito dal responsabile dell'Amministratore di Sistema previa richiesta.
7.8) L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali. In ogni caso, prima di iscriversi, occorre non solo verificare in anticipo se il sito è affidabile ma anche richiedere l'autorizzazione all'Associazione.
7.9) La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
7.10) Per la trasmissione di file all'interno dell'Associazione è possibile utilizzare la posta elettronica, in alternativa ai software di comunicazione interni forniti dall'Associazione stessa, prestando in ogni caso attenzione alla dimensione degli allegati che non devono mai superare i 10 Mb.
7.11) E' obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti web o server ftp non conosciuti).

ART.8) USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI (modalità di connessione alla rete Internet II)
8.1) Il PC abilitato alla navigazione in Internet costituisce uno strumento associazionistico necessario allo svolgimento della propria attività.
8.2) La navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa non è consentita anche se in misura limitata.
8.3) Non possono essere utilizzati modem privati per il collegamento alla rete.
8.4) E' fatto divieto di scaricare software gratuiti (freeware) e shareware prelevato da siti internet, se non espressamente autorizzato dall'Amministratore di Sistema.
8.5) E' fatto divieto di scaricare software non legali, cosiddetti "craccati" ovvero senza valida licenza.
8.6) 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 book (a titolo esemplificativo e non esaustivo, Facebook, Twitter, ecc.) anche utilizzando pseudonomi (o nicknames).
8.7) E' fatto divieto di effettuare transazioni prelevate tramite internet (ad es. acquisti, aste on-line, compravendita di titoli), effettuare scommesse o puntate di gioco d'azzardo, ...).
8.8) In ogni caso, anche in considerazione dell'attività svolta da O.I.P.E.S., l'utilizzo della rete Internet deve essere improntato ai canoni di eticità e, pertanto, è assolutamente vietato l'accesso a siti inappropriati (come, a titolo esemplificativo e non esaustivo, siti pornografici, pedopornografici, di intrattenimento, ecc.). A tali fine l'attività e la navigazione Internet potranno essere regolamentate con strumenti elettronici, attraverso opportuni sistemi di "content-filtering" (cioè appositi sistemi che permettono o meno la visualizzazione di pagine web in Internet) che consentono di bloccare l'accesso degli utenti ai summenzionati siti web inappropriati e volti a limitare/ottimizzare il tempo di navigazione.
8.9) Nel caso in cui i soci e/o collaboratori dovessero per caso entrare in siti pedopornografici saranno tenuti ad informare immediatamente l'Amministratore di Sistema.
8.10) La navigazione internet può essere assoggettata a regole in merito ai tipi di contenuti o vincolata a liste di siti

predefiniti. Vengono inoltre stabilite regole sul blocco di files per i quali è o non è consentito il download oltre all'uso di applicazioni di messaggistica (chat). Per accedere ad internet è pertanto indispensabile avere il proprio identificativo (username e password) il quale, strettamente personale, non deve e non può essere divulgato a terzi.

8.11) I log relativi al traffico telematico vengono conservati per il tempo strettamente necessario "al perseguimento di finalità organizzative, produttive e di sicurezza"; il tempo massimo consentito per la conservazione è disciplinato dall'art. 132 del Codice Privacy e, pertanto, può essere soggetto a successive modificazioni. Queste informazioni sono peraltro accessibili solo all'Amministratore di Sistema e al responsabile del trattamento dei dati e questi dati sono oggetto di periodica cancellazione, nell'ambito delle comuni procedure di manutenzione delle attrezzature hardware e software.

Non si esclude che, in alcuni casi (ad esempio nei salvataggi della posta elettronica), i backup possano archiviare alcuni di questi dati "temporanei". Tale archiviazione è però frutto delle normali attività (obbligatorie per esigenze tecniche o di sicurezza) di backup o di gestione della rete e non può essere considerata come parte di una policy di controllo e di verifica delle attività lavorative.

8.12) Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici o strumenti elettronici (art. 8.7), il datore di lavoro ha previsto di adottare eventuali misure che consentano la verifica di comportamenti anomali. In questo caso è comunque preferito, laddove non diversamente applicabile, un controllo preliminare su dati aggregati (e quindi anonimi) riferiti all'intera struttura associazionistica o a sue aree.

Tale controllo anonimo potrà concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti associazionistici e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso potrà essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.

8.13) Ai sensi dell'art. 13 del Codice della Privacy l'utente si ritiene informato delle politiche che disciplinano l'uso di internet.

ART.9) PROTEZIONE ANTIVIRUS

9.1) E' necessario tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico associazionistico mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc.).

9.2) Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus associazionistico, ove presente.

9.3) Nel caso che il software antivirus rilevi la presenza di un virus, malware, spyware che non è riuscito a ripulire, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare l'accaduto all'Amministratore di Sistema.

9.4) Ogni dispositivo magnetico o di archiviazione di massa (come, a titolo esemplificativo e non esaustivo, chiavette USB, dischi esterni, CD, DVD, ecc.) di provenienza esterna all'associazione dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, malware, spyware non eliminabile dal software, il dispositivo non dovrà essere utilizzato.

ART.10) UTILIZZO DEI TELEFONI FISSI E PORTATILI

10.1) Non è consentito l'uso delle linee telefoniche associazionistiche per motivi privati, se non previa richiesta e conseguente autorizzazione da parte dell'Amministratore di Sistema.

10.2) Nei locali associazionistici e durante l'orario di lavoro non è consentito l'uso smisurato del proprio telefono portatile.

10.3) Non è consentito il trasferimento di dati aziendali sul proprio telefono portatile, se non previa richiesta e conseguente autorizzazione da parte dell'Amministratore di Sistema.

ART.11) SOGGETTI INCARICATI

11.1)L'Associazione ha incaricato anche soggetti appartenenti alle strutture che, occasionalmente, effettuano manutenzione ed assistenza alla rete informatica associazionistica, e precisamente:

- VINATI IMMOBILI SRL. – Brescia

Nell'effettuare controlli sull'uso degli strumenti elettronici, manutenzione o assistenza è evitata qualsiasi interferenza ingiustificata sui diritti e sulle libertà fondamentali di soci/collaboratori, come pure quella di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

ART.12) OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

12.1) E' obbligatorio attenersi alle disposizioni di cui al Regolamento sulle misure minime di sicurezza (Regolamento associazionistico) e al Documento Programmatico sulla Sicurezza.

ART.13) NON OSSERVANZA DELLA NORMATIVA AZIENDALE

13.1) Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari nonchè con le azioni civili e penali previsti dalle seguenti leggi e norme: L. 248/2000, L. 547/1993, art. 171-ter L. 633/1941, artt. 594 e 595 c.p., art. 600-ter c.p. e segg., artt. 615-ter, 615-quater, 615-quinques c.p., artt. 617-quater, 617-quinques, 617-sexies c.p., art. 635.bis c.p., artt. 640 e 640-ter c.p.

ART.14) AGGIORNAMENTO, REVISIONE e DECORRENZA

14.1) Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento tramite comunicazione al responsabile della Sicurezza Informatica.

14.2) Il presente Regolamento è soggetto a revisione con frequenza annuale.

14.2) Tale Disciplinare viene consegnato ai singoli soci, dipendenti e collaboratori, che firmano per ricevuta, e viene applicato in associazione a partire dal giorno_____

O.I.P.E.S.

_____

Per ricevuta

_____

ORGANIZZAZIONE ITALIANA PROFESSIONISTI EDUCAZIONE E SPORT
Via Umberto I, 38 - 27050 Silvano Pietra (PV) - Tel. 0383/378944 - Fax 0383/378947 - e-mail: segreteria@oipes.org - www.oipes.org
Cod. Fiscale: 98113230175 e P. Iva 02564590186