DISCIPLINA UTILIZZO STRUMENTI INFORMATICI

1. SCOPO E APPLICABILITÀ

Il presente documento ha l'obiettivo di regolamentare l'utilizzo degli strumenti informatici assegnati ai soci e alle risorse che operano con continuità presso UNITRE.

2. PRINCIPI DI ATTUAZIONE

L'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo della nostra Associazione deve ispirarsi al principio della diligenza e correttezza, comportamenti che il socio è sempre tenuto ad adottare.

Quindi, ogni utilizzo delle apparecchiature, degli elaboratori, delle reti e dei dati diversi dalle finalità istituzionali deve essere limitato e di natura occasionale. Poiché anche nella normale attività alcuni comportamenti possono mettere a rischio la sicurezza e l'immagine sociale, di seguito vengono richiamate semplici regole procedurali finalizzate non tanto a censurare comportamenti consapevolmente scorretti già di per sé proibiti, ma soprattutto per evitare condotte che inconsapevolmente possano causare rischi alla sicurezza del trattamento dei dati dell'associazione.

A seguito dell'emanazione, da parte del Garante per la Protezione dei Dati Personali, del provvedimento generale del 1 marzo 2007 avente ad oggetto "Linee guida del Garante per posta elettronica e internet[1]" ed al fine di conciliare l'esigenza di tutela della privacy pur garantendo la migliore operatività, UNITRE ha adottato il presente Disciplinare interno che regolamenta, pur nel rispetto dei principi di pertinenza e non eccedenza, le modalità di utilizzo del servizio di posta elettronica sociale, nonché le attività di controllo che UNITRE può legittimamente effettuare per mezzo dei medesimi strumenti tecnologici.

3. REGOLE DA RISPETTARE

3.1 CONTROLLO DEGLI ACCESSI

Ogni utente autorizzato a disporre di dati e di risorse informatiche (pc e telefoni) è assoggettato ad un processo di autenticazione che avviene con la digitazione della password (parola chiave) che deve essere composta di almeno di 8 caratteri e comprendere almeno una lettera maiuscola ed un numero. Essa non deve contenere riferimenti agevolmente riconducibili all'utente (nome o data di nascita propri o dei propri familiari, nome del proprio cane o altri elementi simili). Per mantenere accessi sicuri, la password va modificata ogni sessanta giorni. Le password sono personali e non devono essere divulgate a terzi ed all'esterno dell'associazione e devono essere custodite dall'assegnatario del pc con la massima diligenza.

Rimozione o trasferimento dei diritti di accesso: chi lasci il proprio incarico si assicurerà di annullare la password utilizzata per l'accesso, ovvero di trasferirla a chi gli succederà, a seconda di quale soluzione ha meno impatto sugli aspetti organizzativi.

3.2 POSTA ELETTRONICA

Il servizio di posta elettronica sociale è disponibile ai soci autorizzati. Occorre notare che non si tratta di un servizio in tempo reale, ovvero il tempo fra invio e ricezione di un messaggio non è istantaneo e dipende da molti fattori esterni. L'invio di e-mail con allegati pesanti a mittenti multipli deve essere limitato.
Nell'ambito delle Linee Guida sopra richiamate, UNITRE, rispetto all'utilizzo del servizio di Posta Elettronica ed in osservanza dei principi di pertinenza e non eccedenza, mette a disposizione indirizzi di posta elettronica condivisi per ufficio e/o servizio (ad esempio: info@unitrepino.it, oppure segreteria@unitrepino.it);

L’utilizzo della posta elettronica contribuisce in modo sensibile a rendere la comunicazione tempestiva, efficace ed economica. Il rispetto delle semplici regole richiamate di seguito può aiutare a migliorare ulteriormente l’utilizzo dello strumento:

- L’utilizzo degli strumenti di comunicazione telematici deve fare riferimento a regole organizzative esistenti. In generale ogni comunicazione, inviata o ricevuta che abbia contenuti significativi o contenga impegni per l'associazione, deve essere visionata e autorizzata dalla presidenza o comunque formalizzata nel rispetto delle deleghe attribuite.
- La divulgazione degli indirizzi destinati alla ricezione di comunicazioni ufficiali va limitata a casi specifici.
- È possibile utilizzare la ricevuta di ritorno per avere la conferma della avvenuta lettura del messaggio da parte del destinatario.
- La casella di posta elettronica sociale deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti.
- È sconsigliato l’utilizzo di caselle di posta elettronica sociale per l’invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed espressa autorizzazione da parte della presidenza.
- È facoltà dell’utente avere un proprio indirizzo elettronico presso sistemi esterni WEB; l’utilizzo delle risorse sociali per collegarsi a tale casella di posta elettronica privata è consentito

3.3 STAMPA DI DOCUMENTI RISERVATI

La stampa di documenti riservati deve sempre essere eseguita con estrema cura.

La stampa di documenti confidenziali può essere effettuata anche su stampanti di gruppo avendo cura di non lasciare incustodita la stampante.

Al termine della consultazione, le stampe riservate dovranno essere distrutte.

3.4 ANTIVIRUS E ANTIMALWARE

Tutti i personal computer dispongono di apposito software che:

- protegge in tempo reale il computer e i dati letti/scritti;
- può verificare che le informazioni presenti nei dischi siano libere da virus; aggiorna automaticamente il dizionario dei virus; questa attività viene eseguita ad ogni collegamento alla Intranet sociale;
- gestisce e rende visibile centralmente lo stato dei computer;

I software antivirus non vanno disabilitati.

Qualora si sospetti la presenza di un virus, oppure riscontri un comportamento anomalo del computer, si deve:

- Scollegare immediatamente il computer dalla rete
- Informare la presidenza e/o l’eventuale responsabile dei mezzi informatici fornendo tutte le informazioni disponibili.

3.5 UTILIZZO DEI MEZZI INFORMATICI

L'accesso ai pc sociali è sempre protetto da una password, così come previsto dalle misure minime di sicurezza disciplinate dal Codice della Privacy ed in particolare dall'Allegato B, denominato "Disciplinare tecnico in materia di misure minime di sicurezza".

Costituisce buona regola la periodica pulizia degli 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 che non consenta in modo chiaro ed inequivocabile, l'identificazione dello stato di revisione di un documento.

Il personal computer deve essere spento prima di lasciare gli uffici e comunque protetto nelle pause durante l'orario di lavoro. L'attivazione automatica di uno screen saver con disconnessione automatica dell'utente dopo 10 minuti di inutilizzo è una misura consigliabile per evitare accessi impropri.

L'utente dovrà adottare misure atte ad impedire l'accesso da parte di terzi all'elaboratore incustodito. L'autore di un eventuale utilizzo indebito non sarebbe identificabile a posteriori con possibili ricadute su Unitre e sull'utente incauto.

I fornitori esterni, addetti alla manutenzione di hardware, software e reti, operano in conformità alle presenti direttive, sotto la sorveglianza del responsabile designato.

3.6 UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

L'utilizzo imprudente di alcuni servizi della rete Internet, ancorché nell'ambito della normale attività sociale, può essere fonte di particolari minacce alla sicurezza dei dati e all'immagine sociale.

Seguono alcune semplici regole che devono essere osservate in tale circostanza. Dall'interno della rete sociale, quindi:

- non è consentito scaricare (download e/o upload) file e/o programmi software, anche gratuiti, non aventi attinenza con la propria mansione, e archiviarli su supporti di memorizzazione di massa. Tali supporti sono costituiti dai sistemi di archiviazione dei PC (hard disk), nonché dagli strumenti fisici di archiviazione esterna (CD rom, DVD rom, hd esterni, chiavette di memorizzazione, ecc…).
- è proibita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla presidenza e con il rispetto delle normali procedure per gli acquisti;
- è vietata la partecipazione a Forum non autorizzati, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e la registrazione in guest books anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività sociale;
- è sconsigliato l'uso della rete per accessi a servizi con finalità ludiche o estranei all'attività.
- è, infine, vietato qualsiasi uso improprio (giochi d'azzardo, ecc.) che possa creare nocumento all'associazione.

3.7 CONTROLLI E CONSERVAZIONE DEI DATI

UNITRE ha predisposto il proprio servizio informativo e l'accesso alla rete internet esclusivamente per esigenze organizzative e/o operative.

UNITRE si riserva:

- di effettuare controlli nel rispetto dei principi di pertinenza e non eccedenza, secondo le prescrizioni contenute nel presente disciplinare;
- di verificare comportamenti anomali nel caso in cui un evento dannoso e/o una situazione di pericolo non siano stati impediti con i preventivi accorgimenti tecnici standard;
- di effettuare controlli anonimi causati da un rilevato utilizzo anomalo degli strumenti sociali il cui esito deve essere comunicato tramite avviso generalizzato.

UNITRE non procederà ad effettuare controlli prolungati, costanti e/o indiscriminati.

In merito alla conservazione dei dati, UNITRE adotta le seguenti procedure:

- I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
- In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata da una finalità specifica e comprovata. Il tempo di conservazione deve essere limitato a quanto necessario per raggiungere tale finalità. Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e autorizzato solo in relazione:
    - ad esigenze tecniche o di sicurezza del tutto particolari;
    - all'indispensabilità del dato per l'esercizio o la difesa di un diritto in sede giudiziaria;
    - all'obbligo di ottemperare ad una specifica richiesta dell'autorità giudiziaria e della polizia giudiziaria.

In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati.

3.8 PC PORTATILI

Per loro natura i portatili sono più soggetti a furti e smarrimenti. Durante l'utilizzo in ambienti di lavoro è opportuno assicurarli ad oggetti inamovibili tramite cavo Kensington. Sarà, inoltre, cura dell'assegnatario evitare di lasciare il PC in situazioni rischiose (es.: incustodito in auto) e porre particolare attenzione al back-up periodico dei dati contenuti nel portatile, critici per l'associazione.

In caso di furto o smarrimento il processo da adottare è:

- denunciare l'incidente alle autorità competenti
- fornire copia della denuncia alla segreteria

3.9 TELEFONI, SMARTPHONE, CHIAVETTE DI ACCESSO AD INTERNET

UNITRE fornisce ai soci utilizzatori che ne abbiano necessità, ed esclusivamente per esigenze di servizio, un telefono con relativa SIM. Il telefono deve essere protetto da un codice di blocco e deve richiedere all'accensione il PIN della SIM. Non è ammesso spostare la SIM sociale su dispositivi personali.

Le eventuali chiavette di accesso ad Internet devono essere configurate per richiedere il PIN della SIM dati.

Se il dispositivo mobile lo consente, impostare le funzionalità "Find my Iphone" per IOS oppure l'equivalente servizio di Google per Android.

Nel caso di furto o smarrimento segnalare immediatamente l'accaduto alla presidenza, nel caso il problema si sia verificato fuori dal normale orario di lavoro oppure nel weekend, procedere in modo autonomo richiedendo il blocco del dispositivo al gestore della telefonia (TIM).

In ogni caso In caso di furto o smarrimento il processo da adottare è:

- denunciare l'incidente alle autorità competenti
- fornire copia della denuncia alla segreteria

3.10 DISMISSIONE DEI SUPPORTI

Tutti i supporti magnetici riutilizzabili (cd, dischi e penne USB) contenenti dati riservati devono essere trattati con particolare cautela. Una persona esperta potrebbe infatti, recuperare i dati memorizzati anche dopo la loro cancellazione.

3.11 CLEAR DESK E CLEAR SCREEN

UNITRE promuove per le postazioni di lavoro interne la politica della scrivania pulita.

Questa politica prevede di non lasciare mai giacenti sulla scrivania documenti cartacei contenenti informazioni riservate, per evitare che siano letti, carpiti o anche solo sfogliati da qualche occhio indiscreto. Le informazioni, che dovrebbero essere preferibilmente di tipo elettronico e stampate su carta solo in caso di effettiva necessità, devono sempre essere riposte in un luogo sicuro, ad esempio in un armadio con chiave, quando si lascia la postazione di lavoro.

Anche la scrivania virtuale, il desktop della postazione, deve proteggere le informazioni secondo la politica "Clear Screen", ovvero del desktop pulito.

È necessario evitare, quindi, di lasciare aperti sul desktop del computer documenti riservati; se ci si allontana dalla postazione occorre assicurarsi di bloccarla con lo screen saver protetto da password.

3.12 ATTIVITA' DI FORMAZIONE

UNITRE predispone momenti formativi ed informativi per garantire a tutti gli utenti il massimo aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati e alla sicurezza delle informazioni.