DISCIPLINARE SULLE MISURE DI SICUREZZA DEGLI STRUMENTI INFORMATICI A PROTEZIONE DEI DATI PERSONALI

SCOPO

Il presente disciplinare ha lo scopo di fornire indicazioni per l'utilizzo sicuro ed appropriato delle risorse informatiche (hardware, software, Internet, posta elettronica) date in uso al personale. Il disciplinare si prefigge lo scopo di una gestione controllata, efficace, efficiente e conforme alla normativa tramite:

- l'informazione/formazione di tutto il personale coinvolto;
- l'applicazione del presente disciplinare;
- il monitoraggio del rispetto delle norme impartite con il seguente documento;
- la valutazione del grado di applicazione del presente disciplinare e l'applicazione di opportuni interventi correttivi.

CAMPO DI APPLICAZIONE

Le disposizioni contenute nel presente documento devono essere adottate e rigorosamente osservate all'interno dell'Ente da tutto il personale dipendente e dai soggetti che nelle varie forme collaborano e prestano la loro opera utilizzando uffici e strumentazione dell'ente, al fine di evitare infrazioni alle norme vigenti.

Gli strumenti informatici oggetto del presente disciplinare sono in uso nell'Ente (in proprietà, noleggio, service, comodato o qualsiasi altra forma contrattuale) e sono messi a disposizione degli Utenti al fine di permettere il quotidiano svolgimento delle proprie prestazioni lavorative. Essi sono essenzialmente individuabili quali:

- server, computer, fissi o mobili, tablet e altri apparati mobili, sistemi di identificazione e di autenticazione informatica, smartphone concessi in uso;
- Internet, intranet e altri strumenti di scambio di comunicazioni e file, compresi quelli delocalizzati con tecnologia cloud; apparecchiature informatiche necessarie per l'uso di Internet o intranet;
- posta elettronica;
- qualsiasi altro programma e apparecchiatura informatica destinata a memorizzare o a trasmettere dati e informazioni.

Sono esentati dall'applicazione del presente disciplinare, e limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, gli Amministratori di Sistema formalmente nominati.

SERVIZIO DI ASSISTENZA A MANUTENZIONE

L'Ente rende noto che l'attuale ditta esterna affidataria del servizio di assistenza e manutenzione della rete informatica, nella qualità di Responsabile esterno del trattamento e nella fattispecie in qualità di Amministratore di Sistema, è autorizzata a compiere interventi nel sistema informatico, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi.

Detti interventi potranno anche comportare in qualunque momento, e anche in assenza dell'affidatario l'accesso agli strumenti hardware e di conseguenza anche ai dati trattati da ciascuno, ivi compresi gli archivi su Pc e Server, nonché alla verifica sui siti internet acceduti dagli utenti abilitati.

La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente si applica anche in caso di assenza prolungata od impedimento del dipendente.

La ditta esterna di cui sopra ha inoltre la facoltà di collegarsi, di norma previa autorizzazione dell'Utente, mediante visualizzazione di un indicatore visivo sul monitor che segnala la connessione in remoto del tecnico informatico, e visualizzate in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus informatici in genere. L'intervento di norma viene effettuato esclusivamente su chiamata dell'Utente ma, in caso di oggettiva necessità, ad esempio a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico la cui risoluzione richieda l'accesso ai sistemi affidati al dipendente assente, l'intervento sarà comunque erogato. In quest'ultimo caso, e sempre fatta salva la necessaria

tempestività ed efficacia dell'intervento, verrà data formale comunicazione via e-mail della necessità dell'intervento stesso o dell'avvenuto intervento.

UTILIZZO DI PERSONAL COMPUTER

Per l'utilizzo dei personal computer, sia fissi che portatili, oltre a tablet e altri device similari, l'Utente deve seguire le seguenti indicazioni:

- il computer deve essere spento ogni giorno prima di lasciare gli uffici nonché in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo;
- non è consentito lasciare un elaboratore incustodito acceso o non bloccato; ciò infatti potrebbe permettere l'utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Di conseguenza, qualora ci si allontani dalla propria postazione, occorre bloccare il computer (attivare la schermata di protezione) o disconnettersi;
- i dati devono essere salvati esclusivamente sul server, e non in locale, in modo da poter essere oggetto di backup;
- si possono installare software solamente previa autorizzazione del proprio Responsabile di servizio; in ogni caso i software dovranno essere relativi all'attività lavorativa e provenienti da siti noti e sicuri, previo accertamento inoltre che ciò sia conforme alla licenza d'uso;
- ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, sottoponendoli sempre a scansione antivirus ed avvertendo immediatamente il proprio Responsabile di servizio nel caso in cui siano rilevati virus di qualsivoglia natura;
- non è consentito collegare alla rete informatica personal computer o pc portatili e, più in generale, qualsiasi dispositivo hardware non ascrivibili alla proprietà o altra forma di possesso dell'Ente, salvo specifica autorizzazione del Responsabile del servizio interessato.

DISPOSITIVI ELETRONICI PORTATILI

L'Utente è responsabile dell'integrità dei dispositivi elettronici portatili (computer portatile, tablet, smartphone, supporto di memorizzazione, …) affidatogli dall'Ente e dei dati ivi contenuti.

L'Utente è tenuto a custodirlo con diligenza sia durante l'utilizzo nel luogo di lavoro sia durante i suoi spostamenti. A tali dispositivi si applicano le regole di utilizzo previste per i personal computer.

Nel caso di utilizzo condiviso con altri Utenti, prima della riconsegna occorre provvedere alla rimozione definitiva di eventuali file elaborati contenenti dati personali.

I supporti di memorizzazione, se contenenti dati particolari o giudiziari dovranno essere criptati, al fine di evitare, in caso di furto o di smarrimento, l'accesso ai dati stessi da parte di soggetti non autorizzati.

STAMPANTI E FOTOCOPIATORI

Qualora l'Utente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà aver cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

È fatto divieto di lasciare documenti incustoditi nei fax, nei fotocopiatori e nelle stampanti condivise.

CREDENZIALI DI ACCESSO

Ad ogni Utente "incaricato" sono assegnate o associate individualmente una o più credenziali per l'autenticazione (identificativo e password) necessarie per accedere alle risorse informatiche e alle applicazioni software; l'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo. Al fine di agevolare l'Utente nella corretta gestione delle proprie password, possono essere utilizzati software di password manager.

Le credenziali di autenticazione per l'accesso alla rete aziendale vengono inizialmente assegnate dall'Amministratore di Sistema e successivamente obbligatoriamente reimpostate dal dipendente stesso secondo le modalità operative di seguito meglio specificate.

La credenziale di autenticazione (login) consiste in un codice per l'identificazione dell'Utente (user id), assegnato ed associato ad una parola chiave (password) riservata e modificata dall'Utente al primo accesso. Essa dovrà essere memorizzata, custodita con la massima diligenza e non divulgata.

La password deve:

- essere composta da almeno 12 caratteri;
- non contenere riferimenti all'Utente (es. nome o cognome);
- non essere composte da semplici sequenze di tasti (es. "qwerty"), o da ripetizioni del proprio nome utente (es. "rossirossi");
- non essere utilizzata per accessi a sistemi diversi (es. accesso al sistema operativo, software gestionale, posta elettronica, portali web).

La password di accesso di ciascun Utente dovrà essere reimpostata a cura dell'Utente periodicamente, almeno una volta all'anno. Nel caso fosse possibile inserire tale procedura in automatico sarà cura dell'Utente inserire una nuova password, diversa dalla precedente.

Intervalli di tempo più ravvicinati, secondo i maggiori esperti di sicurezza informatica, produrrebbero effetti negativi incentivando l'Utente ad usare solo banali cambi di password tra la precedente e la nuova, al fine di poterla facilmente ricordare.

Nel caso in cui l'Utente venga a conoscenza del fatto che la password sia stata violata deve procedere senza ritardo ad informare il proprio Responsabile del servizio e l'assistenza tecnica, nonché a sostituire la password ovunque sia stata impostata.

L'Utente deve impostare il blocco schermo automatico che si attivi in caso di inutilizzo della risorsa per un periodo superiore ai 5 minuti.

UTILIZZO DELLA POSTA ELETTRONICA

Il servizio di posta elettronica è un mezzo istituzionale di comunicazione aziendale e il suo utilizzo deve avvenire nel rispetto delle norme in materia di protezione dei dati personali.

La prudenza nella gestione delle e-mail ricevute contribuisce in grande misura alla sicurezza dei dati presenti nei sistemi informativi. Il rispetto delle semplici regole che seguono si rendono quindi necessarie per una adeguata protezione contro gran parte delle attuali minacce:

- diffidare delle e-mail di cui non si conosce l'indirizzo del mittente; in questo caso non aprire mai gli allegati o i programmi ivi contenuti, né selezionare i link indicati;
- anche se il messaggio e-mail sembra provenire da un mittente conosciuto, prestare attenzione al suo contenuto e alla sua "attendibilità", in quanto risulta molto semplice inviare messaggi e-mail a nome di altri; in caso di dubbio contattare (anche telefonicamente) il mittente per verificare l'autenticità del messaggio;
- aprire unicamente i file o i programmi provenienti da fonti affidabili e solo previa verifica con un programma antivirus aggiornato;
- non aprire mai gli allegati ad e-mail provvisti di due estensioni (es. picture.bmp, .exe, .vbs) e non lasciarsi ingannare dall'icona di simili file;
- non rispondere agli spam: rispondere ad un messaggio di spam equivale ad informare lo spammer che l'indirizzo e-mail è valido e quindi questi invierà ulteriori spam oppure metterà il vostro indirizzo a disposizione di altri spammer; particolare attenzione va portata agli spam con l'opzione di "cancellazione dall'elenco" in cui si promette la cancellazione dall'elenco di distribuzione tramite l'invio di una e-mail con un determinato contenuto;
- avvertimenti di pericolo di virus inviati tramite e-mail: nella maggior parte dei casi sono false informazioni; non eseguire mai, in nessun caso, le raccomandazioni ivi contenute; questo con particolare riferimento a cancellazione di file, installazione di un determinato programma, inoltro dell'informazione ai conoscenti;
- in caso di dubbi contattare sempre il proprio Responsabile di servizio.

In caso di assenza prolungata programmata dell'Utente, si raccomanda allo stesso di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate di

un collega che può essere contattata in sua assenza e/o altre modalità utili di contatto della Struttura organizzativa presso cui presta la propria attività lavorativa.

NAVIGAZIONE INTERNET

Gran parte dei pericoli per la sicurezza del sistema informativo vengono corsi durante la navigazione in Internet. Molti di questi pericoli possono essere evitati adottando opportune misure comportamentali, pertanto gli Utenti devono osservare le seguenti indicazioni:

- effettuare l'accesso solamente a siti web sicuri e noti;
- non scaricare mai programmi sconosciuti da Internet prima di averne accertato la provenienza.
- non comunicare mai a nessuno le proprie credenziali di accesso (nome di utente e password), nessun fornitore di servizi serio chiederà la vostra password (nemmeno telefonicamente), anche quando la richiesta appare credibile;
- utilizzare sempre l'apposita notifica di chiusura ("logout") quando si esce da un'applicazione web che abbia richiesto l'introduzione delle proprie credenziali di accesso;
- evitate di rivelare dati personali durante la compilazione di moduli web.

PROTEZIONE DA VIRUS

Le postazioni di lavoro sono protette da software antivirus aggiornato quotidianamente.

Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico. Questa fattispecie può accadere mediante virus o malware, proveniente da dati e/o software importati/installati dall'Utente, che si auto-installano, all'insaputa dell'Utente, all'interno del Pc, infettandolo e diffondendosi nella rete informatica aziendale.

Nel caso in cui il software antivirus rilevi e non disinfetti la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto al proprio Responsabile di servizio.

Ogni dispositivo di memorizzazione esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e nel caso venga rilevato un virus, dovrà essere prontamente consegnato all'assistenza tecnica che provvederà ad effettuare le dovute operazioni di disinfezione.

SMALTIMENTO DEI DISPOSITIVI ELETTRONICI

In caso di smaltimento di dispositivi elettronici contenenti dati personali, l'Utente deve accertarsi che siano fisicamente distrutti ovvero cancellati tramite opportuni software di formattazione approfondita. In ogni caso si rende opportuno consultare il proprio Responsabile di servizio.