Città metropolitana di Venezia

Istruzioni per l'utilizzo delle risorse informatiche e per il trattamento dei dati

Premessa

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto: tali strumenti vanno custoditi in modo appropriato e possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati il furto, il danneggiamento o smarrimento di tali strumenti.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità proprie. In questo contesto la Città metropolitana di Venezia potrà per necessità di sicurezza aziendale e o per esigenze di continuità della normale attività lavorativa, accedere agli archivi di corrispondenza elettronica o ai file di log riservati alla tracciatura degli eventi di connessione.

Utilizzo del personal computer

- é consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal servizio informatica; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o eliminare il contenuto di comunicazioni e/o documenti informatici. Non è consentito collegare al computer in dotazione mezzi di comunicazione propri (es. smartphone);
- i Personal Computer contengono informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere salvato, nemmeno per brevi periodi, in queste unità; l'ente si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.
- sui personal computer non viene effettuato alcun salvataggio dati, pertanto è preferibile, se non obbligatorio per dati importanti, l'utilizzo delle cartelle di rete. Le cartelle di rete hanno regole di accesso legate alle competenze ad alla autorizzazioni di ogni dipendente e vengono quotidianamente salvate .

Utilizzo di internet

- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
- a maggior ragione non è consentito navigare in siti che contengono contenuti contrari alla morale e alle prescrizioni di Legge;
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal servizio informatica Titolare o dal Responsabile del Trattamento e con il rispetto delle normali procedure di acquisto;
- non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato dal servizio informatica Titolare o dal Responsabile;
- non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di "peer to peer;"
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non è permessa la partecipazione durante l'orario di lavoro, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e l'uso di piattaforme "social" anche utilizzando pseudonimi (o nicknames);
- non è consentita la memorizzazione di documenti informatici di natura oltraggiosa .

Utilizzo del servizio di posta elettronica

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- non è consentito utilizzare la posta elettronica aziendale per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente Riservati";
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail-list; solo in questo ultimo caso è possibile, previa autorizzazione per la verifica della validità dell'emittente, iscriversi a servizi di informazione strettamente inerenti all'attività dell'ente;
- non è consentito utilizzare web mail e/o caselle di posta elettronica non appartenenti al dominio o ai domini della città metropolitana di Venezia salvo diversa ed esplicita autorizzazione.

Modalità per elaborare e custodire le password

Le credenziali di autenticazione al dominio, ed in generale ai programmi ed alla banche dati essenziali per l'attività lavorativa, sono assolutamente personali e non cedibili, per nessuna ragione.

Rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria Nomina ad Addetto.

Nel caso in cui sia prevista la figura del custode delle copie credenziali, è necessario trascrivere una copia della propria parola chiave e consegnarla in busta chiusa (meglio se sigillata) all'Addetto od al responsabile incaricato alla loro custodia. Fare riferimento al servizio informatica per i dettagli operativi della procedura.

Elaborare le password seguendo le istruzioni sotto riportate.

Scelta delle password

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

Cosa non fare

- NON rilevare a nessuno la propria password. Lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare risorse altrui o possa farlo a suo nome.
- NON scrivere la password in nessun supporto facilmente accessibile.
- Inserire o rinnovare le password in situazioni di sicurezza, al riparo dalla vista altrui.
- NON scegliere password composte da parole di senso compiuto anche di lingue estere.
- NON usi password che possano in qualche modo essere legate all'addetto come, ad esempio, il suo nome, quello di sua moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

Cosa fare obbligatoriamente

- la password deve essere composta da almeno otto caratteri; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica, con caratteri speciali e distinzione tra caratteri maiuscoli e minuscoli;
- la password per gli amministratori di sistema deve essere impostata ad un numero minimo di caratteri pari a quattordici, con gli stessi criteri del punto precedente;

- l'Addetto deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema;
- la password deve essere modificata dall'Addetto almeno ogni 3 mesi.

Obbligo di non lasciare incustoditi e accessibili gli strumenti elettronici

Non lasciare incustodito e accessibile il computer o più in generale smartphone e apparati di memorizzazione dati in dotazione. È necessario terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare, anche solo per cinque minuti effettuando un log out o mettendo in atto accorgimenti tali per cui il computer non resti incustodito.

Procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi

Il servizio informatico dell'ente deve prevedere automatismi in grado di sostituirsi all'addetto per la protezione dei dati prevedendo di:

- aggiornare con cadenza almeno settimanale gli antivirus installati sui personal computer;
- installare le Patch di aggiornamento dei sistemi operativi e dei programmi utilizzati per il trattamento dati personali, con cadenza annuale che diviene semestrale in caso di trattamenti di dati di categoria particolare;
- assicurare un sistema perimetrale antispam alla posta dell'ente che preveda l'aggiornamento quotidiano delle liste di mail potenzialmente pericolose.

Fattori di incremento del rischio e comportamenti da evitare

- l' uso di software gratuito (trial, freeware o shareware) prelevato da siti Internet o in allegato a riviste o libri non autorizzato in modo scritto dal servizio informatico dell'ente;
- collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
- attivazione degli applets di Java o altri contenuti attivi da siti non istituzionali;
- l'apertura di file attached eseguibili o potenzialmente contenenti script attivi da caselle di posta sconosciute.

Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente che può causare effetti dannosi non solo alla postazione di lavoro ma all'intera rete aziendale. Potenzialmente un virus potrebbe cancellare l' patrimonio informatico dell'ente.

Come prevenire i virus:

In caso di utilizzo di chiavette usb o altri strumenti in grado di trasmettere file al sistema informativo dell'ente devono essere sottoposti a scansione dagli appositi sistemi antivirus. Non interrompere i processi di scansione.

Qualora si abbia il sospetto che il personal computer in dotazione non sia aggiornato o sia stato infettato contattare immediatamente il servizio informatico dell'ente e collaborare con esso trasmettendo le informazioni richieste o ritenute utili.

Se si ricevono messaggi di posta elettronica, normalmente da domini esterni, che avvisano di un nuovo pericolosissimo virus, ignorarlo e cancellarlo. Le mail di questo tipo sono dette con terminologia

anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene da indirizzi noti o istituzionali. Eventuali pericoli di rete verranno segnalati nella intranet aziendale.

Analogamente, diffidare di tutti i messaggi che invitano a "diffondere la notizia quanto più possibile". Tipicamente sono hoax. Anche se sembrano diffondere messaggi sociali o caritatevoli o promettono guadagni miracolosi sono tipicamente hoax, spyware e troyan aventi lo scopo di danneggiare o utilizzare indebitamente le risorse informatiche.

Obbligo di riservatezza e cautela nella comunicazione a terzi di dati e informazioni

Anche informazioni di normale quotidianità aziendale o ritenute non riservate all'interno dell'interscambio tra autorizzati, assumono diversa importanza se comunicate all'esterno a soggetti terzi; per tale motivo va sempre posta attenzione allo scambio di informazioni per assicurate l'adeguata tutela dei dati. La salvaguardia delle informazioni e dei dati, oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo dell'ente, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al suo contenuto e all'attendibilità dell'interlocutore.

Social engineering

Il social engineering è l'insieme delle tecniche psicologiche usate da chi vuole indurci ai propri scopi presentandosi personalmente presso di noi o contattandoci dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'ente o la sua organizzazione e il personale che vi lavora, ma possono arrivare a raggiungere dati anche molto riservati.

Con l'ausilio di messaggi studiati o abili tecniche di persuasione l'aggressore può anche renderci complici inconsapevoli di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia del personale, l'apertura di allegati infetti o la visita di un sito che contiene dialer o altro materiale pericoloso. Rispetto al social engineering via e-mail, uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. Per scavalcare queste precauzioni e quindi lanciare il virus, c'è un modo molto semplice: indurre la vittima, tramite espedienti psicologici a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo. In questo senso l'aggressore potrebbe essere capace di sfruttare i nostri punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo .

E-mail phisching

Un altro scopo degli aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modalità vengono richieste ad esempio password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.

Spesso queste tecniche sono abbinate tra loro e applicate più volte nel tempo sulla stessa vittima

Cosa fare

- non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
- limitatevi a fornire informazioni a interlocutori noti e operanti con voi per disposizione aziendale, nei limiti dei contenuti afferenti all'ambito lavorativo a voi assegnato;

- diffidate di messaggi provenienti da fonte non conosciuta;
- non aprite messaggi provenienti da fonte non conosciuta contenenti allegati;
- non aprite messaggi contenenti allegati sospetti;
- non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati; in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
- in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il Responsabile o il Titolare.

Custodia ed utilizzo dei supporti rimuovibili, contenenti (o meno) dati personali

Una particolare attenzione deve essere dedicata ai supporti rimovibili (es. chiavette USB), contenenti dati particolari, nei seguenti termini:

- I supporti rimovibili (es. chiavette USB), contenenti dati particolari devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
- Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

Dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dalla Città metropolitana di Venezia, sulle misure di sicurezza

Pretendere dal titolare che vengano forniti strumenti per la formazione sulla privacy. In particolare relativamente a:

- profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

Istruzioni generiche per il trattamento dei dati

L’addetto dovrà :

- procedere alla raccolta di dati personali, nelle modalità previste dalle sue mansioni e indicate in apposita informativa;
- consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa di cui agli artt. 13-14 del Reg.to UE 2016/679, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile;

- raccogliere, sempre al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbiano provveduto direttamente il Titolare o il Responsabile, e salvo i casi di esonero previsti dalla stessa legge;
- trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti, secondo quanto espresso nell'informativa e, comunque, in modo lecito e secondo correttezza;

adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate dal Titolare o dal Responsabile, in particolare dovrà:

- per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare rispettando strettamente il proprio profilo di autorizzazione;
- conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
- copie di dati personali su supporti rimuovibili sono permesse solo se parte del trattamento, copie di dati sensibili devono essere espressamente autorizzate dal Responsabile del trattamento o dal Titolare. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento o al Titolare;
- segnalare al servizio informatico eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati; segnalare al responsabile del trattamento eventuali circostanze che rendano necessario l’adozione di misure di sicurezza per evitare l’accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal Titolare o dal Responsabile e secondo le modalità stabilite dai medesimi e dichiarate nell'informativa;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- fornire al Titolare o al Responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al Titolare ed al Responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.