ALLEGATO 2

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

PREMESSA

L'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Comune di Potenza ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

Il custode delle parole chiave riservate, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici* della Comune di Potenza. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso 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. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici aziendali*.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici aziendali* nel caso in cui vengano rilevati virus.
La connessione alla rete dell'organizzazione da fuori deve avvenire esclusivamente mediante connessioni criptate (VPN)

UTILIZZO DELLA RETE
Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Responsabile dei sistemi informatici aziendali* può 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.
Costituisce buona regola la periodica (almeno ogni sei mesi) 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.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.
Il *Responsabile dei sistemi informatici aziendali*deve sistemistipulare un contratto con una società terza, scelta in base alle proprie competenze professionali, per una valutazione periodica della sicurezza delle 'applicazioni web' e delle reti informatiche, di conseguenza i test riguarderanno tutto il sistema informatico. Ad esempio, l'analisi di un portale web inizia testando le diverse funzionalità, per poi concentrarsi sul meccanismo di autenticazione e l'interazione con i database. Segue l'analisi della configurazione del relativo server e tutti gli elementi che lo circondano nella rete, e quindi tutti i dati e le informazioni di proprietà di una organizzazione (PenTest);

GESTIONE DELLE PASSWORD
Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Responsabile dei sistemi informatici aziendali*.
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici aziendali. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Responsabile; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici*, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici*.
Quando le password sono usate come informazioni segrete di autenticazione, selezionare password di qualità con lunghezza minima sufficiente, che siano:

- facili da ricordare
- non basate su qualcosa che qualcun altro possa facilmente indovinare od ottenere utilizzando informazioni relative alla persona, per esempio nomi, numeri di telefono e date di nascita, ecc.;
- non vulnerabili ad attacchi a dizionario (ossia non composte da parole incluse nei dizionari)
- prive di caratteri consecutivi identici, formate da soli caratteri alfanumerici o numerici
- se temporanee, cambiate al primo log-on;

Non usare le stesse informazioni segrete di autenticazione per scopi istituzionali/aziendali e non.

Tener conto sempre della seguente politica delle password:

- forzare l'uso di identificativi utente e password individuali per mantenere la tracciabilità;
- permettere agli utenti di selezionare e cambiare la propria password e includere una procedura di conferma per errori di input;
- forzare la scelta di password di qualità;
- forzare gli utenti a cambiare la loro password al primo log-on;
- forzare un cambio periodico e quando necessario delle password;
- mantenere una registrazione delle password precedentemente usate per prevenire il loro riuso;
- non mostrare le password sullo schermo quando vengono inserite;
- memorizzare i file delle password separatamente dai dati del sistema applicativo;
- memorizzare e trasmettere le password in modo protetto.

UTILIZZO DEI SUPPORTI MAGNETICI
Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

UTILIZZO DI PC PORTATILI
L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici aziendali* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
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.
I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Comune di Potenza deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).
Per la trasmissione di file all'interno di Comune di Potenza è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
È 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).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici aziendali*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici aziendali*.
È tassativamente vietata 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 Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È 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 (o nicknames).
È necessario inoltre:

- chiudere le sessioni attive quando hanno completato l'attività, a meno che non possano essere protette da un appropriato meccanismo di bloccaggio, per esempio screen saver protetto da password;
- effettuare il log-off da applicazioni o servizi di rete quando non più necessari;
- proteggere il computer o i dispositivi mobili, quando non in uso, da un utilizzo non autorizzato con una chiusura a chiave o con un controllo equivalente, per esempio una password di accesso.

BEST PRACTIES DA SEGUIRE

Esaminare quali informazioni sono disponibili nella propria organizzazione per determinare se tutte le informazioni personali sono state raccolte per scopi specifici e se è ancora necessario conservare queste informazioni.

Conservare le informazioni personali solo nei luoghi individuati o comunque inventariare sempre un nuovo archivio informatico o cartaceo.
Effettuare verifiche periodiche o controlli a campione per garantire che le informazioni personali vengano conservate con misure di sicurezza idonee al trattamento, alla probabilità di rischio, al tipo di informazioni contenute, alla sensibilità delle informazioni personali, la quantità e i tipi di informazioni detenute, come vengono trasmessi e a quante persone, in quali formati;
Per evitare divulgazioni improprie, stabilire metodi sicuri per distruggere le informazioni non più necessarie (ad esempio, distruggere file cartacei o eliminare in modo sicuro i record elettronici). Considerare, ad esempio, i **rischi associati allo smaltimento di computer o stampanti** in cui le informazioni personali sono state lasciate sul disco rigido.
Obbligare mediante contratti sottoscritti con atti vincolanti i responsabili esterni a conservare i dati solo per il periodo necessario e comunque a rispettare le norme vigenti in tema di protezione dati personali;
Non condividere mai le informazioni personali con alcun individuo o sito Web a meno che la divulgazione sia prevista per norma e per regolamento.
Se il software di sicurezza del computer visualizza un avviso di sicurezza, prestare attenzione e chiamare l'amministratore di sistema.
Non collegare le unità USB al computer a meno che non si sappia da dove proviene, dove è stata collegata in precedenza e solo se strettamente necessario.
Utilizzare le email e gli indirizzi email in maniera idonea.
Per evitare le truffe via email, tenere sempre presente l'indirizzo email da cui viene inviata l'email
Ogni applicazione web prodotta e utilizzata per i servizi di questo ente e richiede dati personali, deve utilizzare il protocollo "https:" e richiederlo nella barra di navigazione.
Conservare i dati personali cartacei in schedari o armadi chiusi a chiave dove l'accesso è consentito solo alle persone autorizzate;
Clean-desk: la necessità di non lasciare, soprattutto a fine giornata lavorativa, documenti contenenti dati personali e particolare sulla scrivania o comunque alla vista di altre persone non autorizzate.

Dovrebbero essere adottate sia una politica di "scrivania pulita" per documenti ed i supporti di memorizzazione rimovibili, sia una politica di "schermo pulito" per i servizi di elaborazione delle informazioni.

Le politiche di scrivania pulita e di "schermo pulito" dovrebbero tenere in considerazione la classificazione delle informazioni (vedere punto 8.2), requisiti cogenti e contrattuali (vedere punto 18.1) nonché i corrispondenti rischi e gli aspetti culturali dell'organizzazione. Le seguenti linee guida dovrebbero essere considerate:

1. le informazioni di business critiche, per esempio su carta o su supporti di memorizzazione digitale, quando non utilizzate, dovrebbero essere chiuse a chiave (idealmente in cassaforte o armadio o altri mobili con caratteristiche di sicurezza) soprattutto quando l'ufficio è vuoto;
2. non si dovrebbero lasciare collegati computer e terminali o questi dovrebbero essere protetti, quando incustoditi, con un salva-schermo e meccanismi di blocco della tastiera controllati con una password o token o con altri meccanismi similari di autenticazione dell'utente e dovrebbero essere protetti da lucchetti con chiave, password od altri controlli quando non in uso;
3. dovrebbe essere impedito l'uso di fotocopiatrici e di altre tecnologie di riproduzione (per esempio scanner, fotocamere digitali);
4. le stampe contenenti informazioni riservate o classificate dovrebbero essere rimosse immediatamente dalle stampanti.

5. Una politica della scrivania/dello schermo pulito riduce i rischi di accesso non autorizzato, di perdita e di danneggiamento delle informazioni durante e al di fuori del normale orario di lavoro. Le casseforti o altre forme di archiviazione sicura potrebbero anche proteggere le informazioni da disastri quali incendi, terremoti, alluvioni o esplosioni.
6. E da prendere in considerazione l'uso di stampanti con codice PIN, cosi che solo chi ha inviato il documento in stampa possa ritirarlo e solo quando si trovi in prossimità della stampante.

Accesso limitato alle informazioni personali e ai luoghi di lavoro solo alle persone autorizzate o su sorveglianza.
Garantire che le protezioni fisiche e hardware siano sufficienti a proteggere da perdita o furto e da accesso, divulgazione, copia, utilizzo e modifica non autorizzati.
Garantire la responsabilità della sicurezza dei dati: I vari tipi di dati personali dovrebbero essere classificati in modo che sia i lavoratori che i dirigenti capiscano le differenze. Classificando i dati personali, i dipendenti dovrebbero essere a conoscenza di come gestire ciascun tipo e quali tipi sono autorizzati a condividere o diffondere.
Applicare policy ai servizi web e di rete: stabilisce come si dovrebbero gestire problemi come l'accesso remoto e la gestione e la configurazione degli indirizzi IP e le politiche di rilevamento delle intrusioni.
Scansione per le vulnerabilità: È importante trovare eventuali vulnerabilità nell'infrastruttura IT prima degli hacker. Poiché gli hacker analizzeranno le vulnerabilità nel momento stesso in cui vengono scoperte, si dovrebbe avere una routine per controllare regolarmente le proprie reti.
Gestione delle patch: aggiornamenti continui dei sistemi software di base e non.
Criteri di sicurezza dei dati: Avere politiche condivise di gestione e protezione dei firewall, database e antivirus. Configurazione di server e sistemi operativi.
La risposta agli incidenti - Se si verifica una violazione della sicurezza, è importante disporre di misure appropriate per gestirla immediatamente. Ciò include la valutazione e la segnalazione dell'incidente e il modo in cui risolvere i problemi che ne derivano per evitare il ripetersi del problema.
Utilizzo accettabile: I dipendenti dovrebbero avere una politica di utilizzo corretto dei dati e dei sistemi ed è buona prassi fare firmare una politica di utilizzo.
Monitoraggio della conformità: attivare audit interni ed esterni servono a garantire che l'azienda rispetti i vari elementi di politica di sicurezza dei dati. I controlli vanno eseguiti regolarmente.
Monitoraggio e controllo degli account: Gestione e monitoraggio degli accessi ai dati personali. Eliminazione degli account sospesi di persone che erano autorizzate al trattamento. La politica di sicurezza dovrebbe designare specifici membri del team per monitorare e controllare attentamente gli account utente, il che impedirebbe il verificarsi di attività illegale.
Segmentazione dei dati e della rete.

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI
È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

NON OSSERVANZA DELLA NORMATIVA AZIENDALE
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.