enaip LOMBARDIA

IMAGINE LEARN LIVE

REGOLAMENTO PER UNA CORRETTA GESTIONE DEGLI STRUMENTI INFORMATICI

Ad integrazione del regolamento per la gestione dei dati delle persone fisiche

IMAGINE LEARN LIVE

UN ALTRO MODO PER VIVERE LA FORMAZIONE

1. POSTAZIONI

La postazione di lavoro deve essere:
- utilizzata solo per scopi legati alla propria attività lavorativa;
- utilizzata in modo esclusivo dal solo operatore autorizzato;
- protetta, evitando che soggetti non autorizzati possano avere visibilità ed accesso ai dati trattati.

Le regole principali per una corretta gestione delle postazioni sono:
- non utilizzare nelle sedi della Fondazione risorse informatiche private, salvo una preventiva autorizzazione;
- non installare autonomamente alcun software sugli strumenti aziendali;
- non lasciare sulla scrivania informazioni riservate o dati personali su qualunque supporto esse siano archiviate (carta, chiavette USB, …);
- in caso di assenza momentanea bloccare il sistema operativo del proprio computer e, in ogni caso, impostare lo screen saver con password in modo che si attivi dopo 5' di inattività;
- non trasmettere dati personali se non si è assolutamente certi dell'identità del destinatario;
- non utilizzare piattaforme pubbliche, ancorché gratuite (quali WhatsApp, Facebook, Instagram, Telegram, …) per la condivisione di dati personali o informazioni sensibili della Fondazione.

2. PASSWORD

Tutti devono gestire la propria password come segue:
- modificare, alla prima connessione, quella che è stata attribuita di default;
- modificare, almeno ogni 90 giorni, o immediatamente nei casi in cui sia compromessa;
- comporla utilizzando almeno 8 caratteri;
- usare sia lettere che numeri, almeno un carattere maiuscolo ed un carattere speciale (£, $, &, %, …);
- non basare la scelta su informazioni facilmente ricollegabili alla propria persona, ad esempio il nome proprio o quello dei familiari, date di nascita, indirizzi, …;
- mantenerla strettamente riservata e non divulgarla a terzi;
- non permettere ad altri utenti di operare con le proprie credenziali;
- non trascriverla in posti facilmente accessibili a terzi (come post-it sulla scrivania), né lasciarla memorizzata sul proprio computer;
- non comunicarla mai per telefono o via e-mail in chiaro.

3. ANTIVIRUS E COMPORTAMENTI DI SICUREZZA

Gli strumenti assegnati alle persone autorizzate al trattamento dei dati sono protetti da antivirus ma rimangono potenzialmente esposti ad aggressioni di software non conosciuti o di comportamenti inavveduti degli utenti. Per ridurre le probabilità del verificarsi di tali attacchi occorre applicare le seguenti precauzioni:
- controllare che il programma antivirus installato, aggiornato periodicamente ed attivo;
- chiudere correttamente i programmi in uso;
- non aprire file provenienti da fonti sospette ed analizzare gli allegati e-mail con attenzione prima di procedere alla loro apertura;
- non scaricare o installare applicazioni / software in assenza di preventiva autorizzazione;
- porre attenzione ai messaggi di errore del proprio computer;
- usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e internet;
- non modificare le impostazioni del proprio computer;
- spegnere il proprio computer al termine della prestazione, prima di lasciare il lavoro.

Se viene segnalato o si verifica un malfunzionamento del computer, che possa far sorgere il sospetto della presenza di un virus, l'operatore deve tempestivamente informare il sopporto IT.

4. DISPOSITIVI PORTATILI E SMARTPHONE

Un dispositivo portatile (ad esempio: notebook, tablet, smartphone) è estremamente vulnerabile.
Per questo, per poter garantire una sufficiente sicurezza, occorre:
- conservare lo strumento in un luogo sicuro;
- non lasciare il dispositivo incustodito;
- fare attenzione all'uso del dispositivo in pubblico (dati e password potrebbero essere carpiti da terzi).

Una elevata attenzione va data all'uso dello smartphone perché nel caso contenga dati di archivio andrebbe anch'esso protetto: per questo, per poter garantire una sufficiente sicurezza, occorre:
- non utilizzare lo smartphone come archivio di documenti contenenti dati aziendali, soprattutto se sono dati particolari;
- non possono essere create pagine Facebook, Instagram o altri social network contenenti il nome di Enaip Lombardia se non su esplicita autorizzazione della Direzione, che individua e nomina un amministratore responsabile.

5. SOTTOSCRIZIONE

Il mancato rispetto del regolamento o la sua violazione potrà comportare provvedimenti di natura disciplinare o contrattuale, oltre ad azioni civili e penali laddove definiti dalle leggi.
Il presente regolamento è stato predisposto dall'azienda ed è sottoscritto dal soggetto collaboratore al quale ne è consegnata una copia, per presa visione ed accettazione del contenuto.

Nome Cognome	data	Firma per presa visione e accettazione
_____	_____	_____