HANDBOOK
per la Sicurezza delle Informazioni

clariane

LAVORARE OGNI GIORNO GIORNO **IN MODO SEMPLICE E SICURO**

Ogni giorno utilizziamo strumenti digitali e informazioni importanti per il nostro lavoro e per le persone di cui ci prendiamo cura.

Proteggere questi strumenti e queste informazioni non è solo una questione tecnica: è una responsabilità condivisa.

Questo handbook ti accompagna nelle scelte quotidiane, ti aiuta a riconoscere i rischi più comuni e a sapere cosa fare quando qualcosa non ti convince.

Non è un regolamento disciplinare: è una guida pratica, pensata per essere utile anche quando hai poco tempo.

LA SICUREZZA È FATTA DI **ATTENZIONE QUOTIDIANA**

La maggior parte degli incidenti informatici non nasce da comportamenti intenzionali, ma da distrazioni, inconsapevolezza o situazioni poco chiare.

- **Un'email che sembra legittima.**
- **Una richiesta urgente.**
- **Un clic fatto in fretta.**

La sicurezza non chiede perfezione,
ma attenzione, buon senso e collaborazione.

USARE CORRETTAMENTE **I DISPOSITIVI AZIENDALI**

Computer, tablet e smartphone aziendali sono strumenti di lavoro e contengono informazioni da proteggere.

Usali con la stessa cura che useresti per documenti importanti.

Proteggili quando ti sposti, anche fuori dall'orario di lavoro, e segnalane subito eventuali perdite, furti o anomalie.

È importante non modificare autonomamente le impostazioni di sicurezza, né installare software o dispositivi non autorizzati.

Gli strumenti messi a disposizione dall'azienda sono configurati per garantire un livello adeguato di protezione: aggirarli o sostituirli può esporre tutti a rischi inutili.

PASSWORD E ACCESSI: LA TUA PRIMA DIFESA

Le credenziali di accesso sono personali e rappresentano la prima barriera contro accessi non autorizzati.

Usa sempre il tuo account personale e mantieni la password riservata.

Evita password facili o legate alla tua vita privata e non riutilizzarle su servizi esterni.

Bloccare il computer quando ti allontani, anche per pochi minuti, è un gesto semplice ma fondamentale.

Se sospetti che la tua password non sia più sicura, cambiala e avvisa l'IT o la Sicurezza Informatica.

Condividere credenziali, anche "per comodità", espone te e l'azienda a rischi seri.

E-MAIL E MESSAGGI: ATTENZIONE ALLE TRAPPOLE

L'email è uno degli strumenti di lavoro più usati, ma anche uno dei principali canali di attacco.

Prima di aprire un allegato o cliccare su un link, prenditi un momento per osservare il messaggio:

- il mittente è noto e il linguaggio coerente?
- il tono è insolitamente urgente?
- la richiesta è plausibile?

Le truffe informatiche spesso fanno leva sulla fretta o sulla paura.

Se qualcosa non ti convince, fermati e segnala: anche un dubbio può prevenire un incidente.

Ricorda: nessuno dovrebbe chiederti password o informazioni sensibili via e-mail.

NAVIGAZIONE
INTERNET E SOFTWARE

Internet è uno strumento di lavoro potente, ma va usato con responsabilità.

Utilizza solo software autorizzati dall'azienda e presta attenzione ai siti che visiti.

Scaricare programmi o contenuti da fonti non affidabili può introdurre virus o malware nei sistemi aziendali.

Se hai bisogno di strumenti specifici per il tuo lavoro, chiedi supporto all'IT o alla Sicurezza Informatica: esistono canali corretti per farlo.

PROTEGGERE
DATI E DOCUMENTI

I dati aziendali, e in particolare quelli relativi a persone, pazienti e colleghi, devono essere trattati con riservatezza.

Condividi le informazioni solo con chi ne ha reale necessità e utilizza sempre gli strumenti aziendali ufficiali.

Evita di salvare documenti di lavoro su dispositivi personali o di inviarli tramite canali non autorizzati.

Anche l'attenzione fisica conta: non lasciare documenti riservati incustoditi e presta attenzione a chi può vedere il tuo schermo.

POSTA ELETTRONICA AZIENDALE

L'email aziendale è uno strumento professionale.

Va utilizzata principalmente per comunicazioni di lavoro, facendo attenzione ai destinatari e ai contenuti.

Messaggi personali ricevuti per errore devono essere cancellati.

Le comunicazioni di lavoro non devono essere inoltrate su account personali o salvate su dispositivi non aziendali, salvo autorizzazioni specifiche.

QUANDO QUALCOSA NON VA: **SEGNALARE È LA SCELTA GIUSTA**

Un incidente informatico può capitare a chiunque.

E-mail sospette, comportamenti anomali, perdita di dispositivi, dubbi su accessi o sicurezza: tutto questo va segnalato subito.

Non è un errore chiedere aiuto.

Non è una colpa segnalare un problema.

Al contrario, segnalare tempestivamente permette di limitare i danni e proteggere tutti e tutte.

IN CASO DI DUBBIO

Se non sei sicuro di cosa fare, fermati un attimo e chiedi.

Il team IT e la Sicurezza Informatica sono a disposizione per supportarti.

La sicurezza delle informazioni funziona solo se ognuno fa la sua parte, ogni giorno.

Grazie per il tuo contributo.

clariane