# Politica per la Sicurezza delle Informazioni per i Fornitori

## Politica per la Sicurezza delle Informazioni

Il **FORMEDIL BENEVENTO Formazione e Sicurezza** implementa e mantiene un Sistema di Gestione delle Informazioni sicuro seguendo i requisiti specificati nella Norma UNI CEI EN ISO/IEC 27001:2017, così da garantire:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. **Controllo**: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità**: garantire una provenienza affidabile dell'informazione;
6. **Privacy**: garantire la protezione ed il controllo dei dati personali.

La mancanza di adeguati livelli di sicurezza delle informazioni può comportare il danneggiamento dell'attività del FORMEDIL BENEVENTO, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica, finanziaria e di immagine dell'azienda e della filiera sottostante.

L'impegno della direzione del FORMEDIL BENEVENTO, che si richiede applicazione anche da parte dei fornitori, si attua tramite la definizione di una struttura organizzativa adeguata a:

- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento della Sicurezza delle Informazioni;
- controllare che la politica per la Sicurezza delle Informazioni sia integrata in tutti i processi aziendali e che le procedure ed i controlli siano sviluppati coerentemente ed efficacemente;
- monitorare l'esposizione alle minacce per la sicurezza delle informazioni;
- attivare programmi per diffondere la consapevolezza e la cultura sulla sicurezza delle informazioni.

Gli obiettivi generali del FORMEDIL BENEVENTO che i fornitori dovranno a loro volta perseguire, sono quindi:

- garantire i migliori standard, ottimizzando e razionando i processi e gli strumenti aziendali;
- garantire l'efficacia delle procedure e controlli per la Sicurezza delle Informazioni;
- garantire la soddisfazione del FORMEDIL BENEVENTO in relazione alla quantità delle informazioni.

Il fornitore deve assicurare che tutto il personale deve operare per il raggiungimento degli obiettivi di sicurezza nella gestione delle informazioni e deve impiegare le tecnologie più adeguate a garantire il rispetto della presente politica.

## Requisiti di Sicurezza delle Informazioni per i fornitori

Lo scambio di documenti e informazioni tra il FORMEDIL BENEVENTO e il Fornitore deve avvenire: per le informazioni riservate tramite e-mail come allegati in cartelle criptate con password; in entrambi i casi, sarà cura del FORMEDIL BENEVENTO fornire, attraverso canali differenti, riferimenti e credenziali alla persona indicata i NDA (o comunque autorizzata allo scambio di dati), via e-mail per tutti gli altri documenti quali informazioni non riservate etc.

Le persone che potranno ricevere informazioni dal FORMEDIL BENEVENTO, ad eccezione quelle pubbliche, sono quelle indicate nell'NDA se sottoscritto tra le parti o diversamente autorizzate da entrambi le parti. Il fornitore si impegna ad attuare soluzioni per la protezione da attività fraudolente, da dispute contrattuali, da divulgazioni e da

modifiche non autorizzate. In caso di necessità di accesso agli asset del FORMEDIL BENEVENTO da parte del fornitore, lo stesso dovrà essere preventivamente autorizzato e informato delle modalità di utilizzo degli stessi, cui dovrà attenersi scrupolosamente e sarà soggetti ai controlli previsti dalle politiche del FORMEDIL BENEVENTO.
Per i fornitori associati ai servizi e ai prodotti della filiera di fornitura per l'ICT, il fornitore deve impegnarsi a rispettare i requisiti del FORMEDIL BENEVENTO per affrontare i rischi relativi alla sicurezza delle informazioni, richiedendo preventivamente al FORMEDIL BENEVENTO copia delle Politiche Applicabili.

## Monitoraggio e riesame dei servizi erogati dal fornitore

Al fine di avere una visibilità complessivamente sufficiente su tutti gli aspetti di sicurezza relativi alle informazioni critiche o alle strutture di elaborazione delle informazioni, il FORMEDIL BENEVENTO monitora i livelli di prestazione del servizio ricevuto al fine di verificare il rispetto degli accordi. Potranno essere condotti audit ai propri fornitori, congiuntamente al riesame dei rapporti di fornitura.

## Gestione degli accessi alla rete ed ai servizi si rete

Qualora il servizio richiesto al fornitore richieda di operare all'interno della rete del FORMEDIL BENEVENTO, allo stesso verrà fornito l'accesso con le seguenti modalità e solo per i servizi ai quali sono stati specificatamente autorizzati dai singoli accordi con il FORMEDIL BENEVENTO:
• Il fornitore dovrà comunicare il nominativo degli operatori che saranno preventivamente approvati dal FORMEDIL BENEVENTO per operare sulla rete
• Agli stessi verrà comunicata una password verbalmente, che non dovrà essere modificata.

## Gestione dei log

L'utente (operatore del fornitore) è soggetto al controllo dei Log da parte del personale ICT del FORMEDIL BENEVENTO.

## Gestione delle password

Gli utenti si impegnano a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso indicati all'interno di questo documento. La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno dell'organizzazione. Gli utenti devono prestare attenzione a fornire le proprie credenziali di accesso, rispondere ad e-mail sospette e/o cliccare sui link durante la navigazione web (o nella mail) al fine di contrastare possibili frodi informatiche (come il phishing, il furto di identità etc.).
Ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account. Qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, l'utente dovrà segnalarlo al FORMEDIL BENEVENTO.
Per la conservazione sicura delle credenziali di accesso è consigliabile evitare di memorizzarle su documenti cartacei o file conservati all'interno della postazione di lavoro.

## Accessi fisici

L'azienda ha predisposto un sistema di controllo perimetrale, con varchi di accesso per proteggere le aree che contengono informazioni critiche e strutture di elaborazione. Al fine di proteggere e limitare l'accesso ad aree che contengono informazioni critiche l'azienda ha predisposto vari sistemi anti-intrusione, il cui layout sono ad uso esclusivo del FORMEDIL BENEVENTO.

## Sanzioni

Il mancato od il ritardato adempimento di quanto previsto dalla presente politica aziendale e/o dal contratto stipulato tra le parti, che dovessero provocare dei danni, comporteranno il conseguente obbligo di risarcimento dei danni in favore del FORMEDIL BENEVENTO oltre alle eventuali sanzioni amministrative pecuniarie e/o penali previste dal GDPR 2016/679 e/o dalla normativa vigente.

Benevento, 05.10.2026

Il Presidente