NEWMEDIAWEB S.R.L. — BLUWIFI

POLITICA PER LA QUALITÀ E PER LA SICUREZZA DELLE INFORMAZIONI

Sistema di Gestione Integrato — UNI EN ISO 9001:2015 | UNI CEI EN ISO/IEC 27001:2024

Con applicazione delle linee guida ISO/IEC 27017:2026 e ISO/IEC 27018:2025 — Revisione 2.2 del 9 settembre 2026

1. Chi siamo

NEWMEDIAWEB S.R.L. (P. IVA 06069670823), che opera nel mercato della connettività con il marchio registrato BluWifi, è un operatore di comunicazioni elettroniche iscritto al Registro degli Operatori di Comunicazione (ROC) e un fornitore di servizi IT. L'Organizzazione ha sede in Via Giordano Bruno 7, 90018 Termini Imerese (PA).

L'attività si articola su quattro linee di business integrate: fornitura di accesso a Internet come Internet Service Provider, su rete propria FWA e in rivendita di servizi FTTH/FTTO di operatori wholesale; fornitura e installazione di prodotti informatici e di impianti tecnologici, con vendita e noleggio di articoli per ufficio; progettazione, erogazione e gestione di servizi IT in cloud e managed services; realizzazione e gestione di infrastrutture di rete, comprendenti reti WiFi ad accesso pubblico e sistemi di videosorveglianza urbana.

2. Campo di applicazione

Erogazione di servizi di accesso a Internet (ISP) tramite rete propria FWA e operatori wholesale di servizi FTTH/FTTO. Fornitura e installazione di prodotti informatici (HW/SW) e impianti tecnologici, compresa la vendita e il noleggio di articoli per ufficio. Progettazione, erogazione e gestione di servizi IT in cloud e managed services. Ai fini del Sistema di Gestione per la Sicurezza delle Informazioni il campo di applicazione è integrato dalla clausola «con l'applicazione dei controlli delle linee guida ISO/IEC 27017:2026 e ISO/IEC 27018:2025», che non si applica al Sistema di Gestione per la Qualità.

La presente Politica si applica a tutte le attività, i processi e le risorse dell'Organizzazione rientranti nel campo di applicazione sopra definito, inclusi i servizi cloud erogati ai clienti business, i servizi di connettività su rete propria e in rivendita e i servizi gestiti per conto di enti pubblici.

Ai fini della sicurezza delle informazioni l'Organizzazione riveste un duplice ruolo in ambito cloud: Cloud Service Provider verso i propri clienti business, ai quali eroga risorse virtuali, backup e monitoraggio; Cloud Service Customer verso il fornitore dell'infrastruttura di virtualizzazione sulla quale il servizio è realizzato. Entrambi i ruoli sono considerati nell'applicazione delle linee guida ISO/IEC 27017:2026.

3. Dichiarazione della Direzione

La Direzione di NEWMEDIAWEB S.R.L. si impegna a erogare servizi IT e di connettività di qualità elevata, affidabili, sicuri e conformi ai requisiti normativi applicabili. Questo impegno si concretizza nel mantenimento e nel miglioramento continuo del Sistema di Gestione Integrato per la Qualità e per la Sicurezza delle Informazioni, conforme alle norme UNI EN ISO 9001:2015 e UNI CEI EN ISO/IEC 27001:2024, con applicazione delle linee guida ISO/IEC 27017:2026 per i servizi cloud e ISO/IEC 27018:2025 per la protezione dei dati personali in cloud.

4. Principi fondamentali

4.1 Qualità e orientamento al cliente

- Comprendere e soddisfare i requisiti e le aspettative dei clienti, business e retail
- Garantire la continuità e l'affidabilità dei servizi erogati con livelli di servizio definiti nella Carta dei Servizi e nelle Condizioni Generali di Contratto, monitorati nel tempo
- Raccogliere e analizzare il feedback dei clienti per il miglioramento continuo
- Gestire reclami e non conformità con tempestività ed efficacia

4.2 Sicurezza delle informazioni

- Proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite dall'Organizzazione e per conto dei clienti

- Adottare misure di sicurezza proporzionate al rischio, in conformità agli standard internazionali
- Garantire la sicurezza dei servizi cloud erogati ai clienti secondo le linee guida ISO/IEC 27017:2026, nel duplice ruolo di fornitore verso i clienti e di cliente verso il fornitore di infrastruttura
- Proteggere i dati personali trattati nell'ambito dei servizi cloud e dei servizi di connettività secondo le linee guida ISO/IEC 27018:2025 e il Regolamento (UE) 2016/679
- Gestire gli incidenti di sicurezza con procedure documentate, assicurando la notifica alle autorità competenti nei termini previsti dalla normativa NIS2 (D.Lgs. 138/2024), per la quale l'Organizzazione è registrata sul portale dell'Agenzia per la Cybersicurezza Nazionale

4.3 Conformità normativa

- Rispettare tutti i requisiti cogenti applicabili all'attività di operatore di comunicazioni elettroniche e di fornitore di servizi IT: UNI EN ISO 9001:2015, UNI CEI EN ISO/IEC 27001:2024, D.Lgs. 138/2024 (NIS2), Regolamento (UE) 2016/679 (GDPR), D.Lgs. 259/2003 (Codice delle comunicazioni elettroniche), delibere AGCOM e obblighi connessi all'iscrizione al ROC
- Mantenere aggiornata la conformità al variare del quadro normativo di riferimento

4.4 Miglioramento continuo

- Condurre audit interni periodici per verificare l'efficacia del Sistema di Gestione Integrato, garantendo l'indipendenza dell'auditor rispetto al processo auditato
- Definire e monitorare obiettivi misurabili per la qualità e per la sicurezza delle informazioni
- Analizzare le non conformità e attuare azioni correttive efficaci
- Sottoporre il Sistema di Gestione a riesame periodico da parte della Direzione

4.5 Gestione dei rischi

- Identificare, valutare e trattare i rischi che potrebbero compromettere la qualità dei servizi o la sicurezza delle informazioni
- Adottare un approccio proattivo alla gestione dei rischi, individuando le opportunità di miglioramento
- Garantire la continuità operativa attraverso backup verificati, ridondanza dei collegamenti e piani di ripristino

4.6 Personale e competenze

- Assicurare che il personale possegga le competenze necessarie per svolgere le proprie attività in modo sicuro e di qualità
- Promuovere la consapevolezza in materia di qualità e di sicurezza delle informazioni attraverso formazione periodica documentata
- Vincolare alla riservatezza tutto il personale e i collaboratori con accesso ai dati

4.7 Gestione dei fornitori

- Selezionare e valutare i fornitori critici sulla base di criteri oggettivi e ponderati di qualità e di sicurezza
- Richiedere ai fornitori che trattano dati per conto dell'Organizzazione adeguate garanzie di sicurezza e, ove applicabile, accordi sul trattamento dei dati personali
- Monitorare le prestazioni dei fornitori critici e rivalutarli periodicamente, adottando misure specifiche di trasparenza nei casi di rapporti con parti correlate

5. Principi di sicurezza adottati

Nell'attuazione della presente Politica l'Organizzazione adotta i seguenti principi, dettagliati nella documentazione interna del Sistema di Gestione per la Sicurezza delle Informazioni.

- Need-to-know e minimo privilegio: l'accesso alle informazioni e ai sistemi è limitato a quanto necessario per il ruolo ricoperto

- Difesa in profondità: i controlli sono articolati su più punti di applicazione lungo il percorso dei dati, dalla frontiera della rete ai singoli servizi
- Accessi amministrativi controllati: la gestione dei sistemi è consentita soltanto da reti autorizzate e, dall'esterno, esclusivamente attraverso canali cifrati dedicati; non esistono percorsi di amministrazione aperti su Internet
- Protezione delle postazioni e della posta elettronica mediante strumenti antivirus e filtri antispam aggiornati
- Autenticazione a più fattori sugli accessi amministrativi che la rendono disponibile, con estensione progressiva pianificata
- Backup verificati: le copie di sicurezza degli ambienti che erogano i servizi sono sottoposte a test di ripristino documentati
- Monitoraggio continuo della rete e degli apparati, con sorveglianza attiva ventiquattro ore su ventiquattro
- Segregazione dei clienti: le risorse assegnate a ciascun cliente nei servizi cloud sono separate logicamente
- Tracciabilità: segnalazioni, guasti e incidenti sono registrati e gestiti su piattaforma, con evidenza delle fasi di lavorazione

6. Comunicazione e disponibilità

La presente Politica è approvata dalla Direzione e riesaminata almeno annualmente; è comunicata a tutto il personale e ai collaboratori con accesso ai sistemi; è disponibile ai clienti, ai fornitori e alle altre parti interessate che ne facciano richiesta ed è pubblicata sul sito www.bluwifi.it.

Gli obiettivi specifici per la qualità e per la sicurezza delle informazioni, con i relativi indicatori e valori attesi, sono definiti nella documentazione del Sistema di Gestione e monitorati nel riesame periodico della Direzione. Gli obiettivi di qualità dei servizi di comunicazione elettronica e i risultati conseguiti sono pubblicati su questo sito nelle pagine dedicate.

Davide Campisi Amministratore Unico Alta Direzione / RQ / RSGI Termini Imerese, 9 settembre 2026	Ezio Piraino Responsabile del Sistema di Gestione Termini Imerese, 9 settembre 2026