

Politica aziendale per i servizi ISP

Qualità del servizio sicurezza delle reti e attenzione al cliente

Società: Global Com Basilicata Srl

Marchio commerciale: globby.it

Versione: 1.0 | Data di emissione: 03.01.2026

Approvata da: Amministratore Unico Global Com Basilicata Srl

Modello da personalizzare e sottoporre ad approvazione prima dell'adozione. I principi seguenti definiscono gli indirizzi per la qualità dei servizi, la sicurezza e la gestione dei rapporti con i clienti.

1 Finalità

Global Com Basilicata Srl fornisce servizi di connettività e telecomunicazioni con l'obiettivo di garantire affidabilità, sicurezza, trasparenza e assistenza qualificata. La presente politica guida le attività aziendali e si applica al personale, ai collaboratori e ai fornitori coinvolti nell'erogazione dei servizi.

2 Qualità e continuità dei servizi

L'azienda si impegna a:

- Monitorare la disponibilità e le prestazioni delle infrastrutture di rete.
- Pianificare manutenzioni e aggiornamenti per ridurre disservizi e interruzioni.
- Dimensionare la capacità di rete in funzione della crescita e dell'utilizzo dei servizi.
- Adottare, dove previsto e tecnicamente possibile, soluzioni di ridondanza e collegamenti di backup.
- Gestire i guasti secondo priorità definite, considerando impatto, estensione e impegni contrattuali.

Gli eventuali livelli di servizio garantiti sono definiti nei contratti e negli accordi applicabili al singolo cliente.

3 Sicurezza delle reti e dei sistemi

L'azienda protegge le infrastrutture attraverso misure tecniche e organizzative proporzionate ai rischi, tra cui:

- Accessi individuali e autorizzazioni limitate alle esigenze operative.
- Autenticazione a più fattori per gli accessi amministrativi, ove disponibile.
- Separazione delle reti di gestione dalle reti destinate ai clienti.
- Aggiornamento dei sistemi e gestione delle vulnerabilità.
- Backup delle configurazioni e verifica periodica delle procedure di ripristino.
- Registrazione e controllo degli accessi e degli eventi rilevanti.

Le credenziali aziendali devono essere custodite con strumenti approvati e non devono essere condivise tramite canali non autorizzati.

4 Protezione dei dati e riservatezza

Il personale tratta i dati dei clienti e le informazioni aziendali esclusivamente per finalità autorizzate e pertinenti alle proprie mansioni. L'azienda definisce modalità di accesso, conservazione e cancellazione dei dati, in coerenza con gli obblighi applicabili. Eventuali accessi non autorizzati, perdite o divulgazioni devono essere segnalati tempestivamente al referente designato.

5 Rapporti con i clienti

Global Com Basilicata Srl promuove relazioni fondate su correttezza e chiarezza, impegnandosi a:

- Comunicare in modo comprensibile prezzi, caratteristiche, condizioni e limiti dei servizi.
- Fornire informazioni sulle tecnologie disponibili e sulla copertura verificata.
- Registrare le richieste di assistenza e seguirle fino alla chiusura.
- Aggiornare i clienti sullo stato dei disservizi rilevanti.
- Gestire i reclami con imparzialità e tracciabilità.

Le comunicazioni commerciali devono essere coerenti con il servizio effettivamente offerto e con le condizioni contrattuali.

6 Gestione di guasti e incidenti

Ogni guasto o incidente deve essere registrato attraverso gli strumenti aziendali, indicando almeno:

- Data e ora di rilevazione.
- Servizi e clienti interessati.
- Gravità e priorità assegnate.
- Attività svolte e responsabile della gestione.
- Ora di ripristino ed eventuali azioni preventive.

Gli eventi con impatto significativo devono essere comunicati al Responsabile Tecnico e alla Direzione. Quando necessario, viene svolta un'analisi delle cause per ridurre il rischio di ricorrenza.

7 Modifiche alle infrastrutture

Le modifiche che possono influire sull'erogazione dei servizi devono essere valutate e autorizzate dal referente competente. Prima dell'intervento devono essere definiti il backup delle configurazioni, le verifiche successive e una procedura di ripristino. Gli interventi urgenti devono essere documentati appena conclusa la fase di emergenza.

8 Personale e fornitori

L'azienda promuove la formazione tecnica e la consapevolezza sulla sicurezza. Dipendenti, collaboratori e fornitori devono rispettare le procedure aziendali, tutelare la riservatezza delle informazioni e segnalare tempestivamente anomalie o situazioni di rischio. Gli accessi dei fornitori devono essere autorizzati, limitati e revocati al termine delle attività.

9 Responsabilità

Le responsabilità sono assegnate secondo l'organizzazione aziendale.

Ruolo	Responsabilità principali
Direzione	Approva la politica e mette a disposizione le risorse necessarie.
Responsabile Tecnico	Coordina la gestione della rete, la continuità operativa e gli interventi tecnici.
Referenti designati	Gestiscono gli ambiti assegnati, inclusi sicurezza, dati personali e assistenza.
Personale e collaboratori	Applicano le procedure e segnalano anomalie e incidenti.

10 Verifica e miglioramento

L'azienda valuta periodicamente l'efficacia delle proprie attività attraverso indicatori quali disponibilità dei servizi, tempi di presa in carico e ripristino, guasti ricorrenti, reclami e risultati delle prove di recupero dei backup. La presente politica viene riesaminata almeno annualmente e in occasione di cambiamenti significativi dell'organizzazione, delle infrastrutture o dei servizi.

La Direzione

[Nome e cognome]

[Firma e data]

La presente politica va affiancata a procedure operative, contratti, Carta dei Servizi e documentazione privacy pertinenti.