

POL-01 Politica Integrata per Qualità, Sicurezza delle Informazioni e Protezione dei Dati Personali

Codice	POL-01
Versione	1
Emissione	15/01/2026
Stato	Approvato
Approvato da	Direzione
Classificazione:	Pubblico

1. Scopo

La presente Politica Integrata stabilisce indirizzi, principi e impegni generali con cui l'Organizzazione WT SRLS governa la qualità dei servizi, la sicurezza delle informazioni e la protezione dei dati personali, in conformità ai requisiti delle norme **UNI EN ISO 9001, ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018**.

La presente Politica costituisce la dichiarazione di intenti della Direzione e il riferimento generale per l'impostazione, il mantenimento e il miglioramento continuo del sistema di gestione integrato.

La presente Politica fornisce il quadro di riferimento per la definizione, il riesame e l'aggiornamento degli obiettivi per la qualità, la sicurezza delle informazioni e la protezione dei dati personali.

2. Principi generali

L'Organizzazione riconosce qualità, sicurezza delle informazioni e protezione dei dati quali elementi essenziali per la continuità operativa, l'affidabilità dei servizi, la tutela delle parti interessate e lo sviluppo delle proprie attività.

L'Organizzazione adotta i seguenti principi guida:

- orientamento ai requisiti del cliente e delle parti interessate rilevanti;
- conformità ai requisiti applicabili di natura legale, regolamentare, contrattuale e organizzativa;
- protezione delle informazioni secondo i principi di **riservatezza, integrità e disponibilità**;
- protezione dei dati personali secondo principi di liceità, correttezza, trasparenza, pertinenza e minimizzazione;
- gestione dei rischi e delle opportunità in coerenza con il contesto e con gli obiettivi aziendali;
- attribuzione chiara di ruoli, responsabilità e autorità;
- sviluppo della competenza, della consapevolezza e della responsabilità delle persone;
- miglioramento continuo dei processi, dei servizi e delle misure di controllo.
- L'organizzazione rende disponibile la politica alle parti interessate sul proprio sito web e/o comunque su richiesta.

3. Impegni della Direzione

La Direzione:

- approva, sostiene e diffonde la presente Politica;
- definisce obiettivi coerenti con la presente Politica e ne verifica periodicamente il raggiungimento;
- assicura risorse, ruoli, responsabilità e autorità necessari al funzionamento del sistema di gestione integrato;
- assicura che rischi e opportunità siano individuati, valutati e trattati secondo criteri coerenti e documentati;
- assicura il rispetto dei requisiti del cliente e dei requisiti applicabili ai servizi erogati;
- persegue l'aumento della soddisfazione del cliente;
- assicura il riesame periodico dell'adeguatezza, dell'efficacia e dell'allineamento del sistema di gestione rispetto al contesto e agli indirizzi strategici;
- assicura il miglioramento continuo delle prestazioni, dei processi e dei controlli adottati.

4. Impegni per la qualità

L'Organizzazione:

- determina il contesto in cui opera e le esigenze delle parti interessate rilevanti;
- gestisce i propri processi in modo pianificato, controllato e coerente con gli obiettivi definiti;
- definisce, attua e monitora obiettivi di qualità;
- assicura il rispetto dei requisiti applicabili ai prodotti e ai servizi;
- presidia la qualità dei servizi erogati e la gestione delle non conformità;

- misura i risultati conseguiti e attua le necessarie azioni correttive e di miglioramento;
- persegue l'aumento della soddisfazione del cliente.

5. Impegni per la sicurezza delle informazioni

L'Organizzazione:

- identifica le informazioni e le risorse rilevanti per il proprio operato e ne assicura adeguata protezione;
- definisce e applica misure di sicurezza coerenti con i rischi individuati;
- disciplina accessi, autorizzazioni e responsabilità secondo criteri di necessità operativa e protezione adeguata;
- assicura continuità, disponibilità, ripristino e resilienza dei servizi e delle informazioni rilevanti;
- gestisce eventi, incidenti, vulnerabilità e cambiamenti in modo controllato e tracciato;
- verifica periodicamente l'efficacia dei controlli adottati e dispone le necessarie azioni correttive e di miglioramento.

6. Impegni per i servizi cloud

In conformità a **ISO/IEC 27017** , **ISO/IEC 27018**, l'Organizzazione governa l'uso e la fornitura di servizi cloud mediante criteri definiti di sicurezza, controllo e responsabilità.

L'Organizzazione:

- definisce ruoli e responsabilità relativi ai servizi cloud;
- integra i rischi specifici dei servizi cloud nei processi di valutazione e trattamento del rischio;
- definisce requisiti di sicurezza e continuità per i servizi cloud utilizzati o erogati;
- seleziona, qualifica, gestisce e riesamina i fornitori di servizi esterni secondo criteri definiti;
- mantiene il controllo sui processi affidati all'esterno che influenzano qualità, sicurezza e conformità.

7. Impegni per la protezione dei dati personali

In conformità a **ISO/IEC 27018 ed al Regolamento UE 2016/679 (GDPR)**, l'Organizzazione tratta i dati personali secondo criteri di protezione, riservatezza, trasparenza e controllo.

L'Organizzazione:

- tratta i dati personali esclusivamente per finalità determinate, legittime e pertinenti;
- applica misure organizzative e tecniche adeguate alla natura dei dati e dei trattamenti svolti;
- limita il trattamento ai dati necessari e ai tempi di conservazione definiti;
- assicura controllo degli accessi, riservatezza e gestione appropriata degli eventi che incidono sulla protezione dei dati;
- disciplina i rapporti con clienti, utenti, fornitori e altre parti coinvolte nel trattamento dei dati personali secondo requisiti chiari e verificabili.

8. Persone, competenze e consapevolezza

L'Organizzazione riconosce il ruolo centrale delle persone nel conseguimento degli obiettivi di qualità, sicurezza delle informazioni e protezione dei dati.

L'Organizzazione:

- assegna compiti, responsabilità e autorità in modo chiaro;
- assicura formazione, informazione e consapevolezza adeguate;
- richiede il rispetto degli obblighi di riservatezza, correttezza e protezione delle informazioni;
- richiede la segnalazione tempestiva di criticità, anomalie, non conformità ed eventi di sicurezza.

9. Conformità e miglioramento continuo

L'Organizzazione mantiene la conformità ai requisiti applicabili e verifica in modo periodico idoneità, adeguatezza ed efficacia del sistema di gestione integrato mediante monitoraggi, audit interni, riesami e azioni correttive.

L'Organizzazione utilizza i risultati delle attività di controllo e valutazione per eliminare le cause delle criticità, prevenire il loro ripetersi e rafforzare la capacità di erogare servizi affidabili, sicuri e conformi.

10. Diffusione e riesame

La presente Politica è approvata dalla Direzione, comunicata, compresa e applicata all'interno dell'Organizzazione ed è resa disponibile alle parti interessate pertinenti.

La presente Politica è riesaminata periodicamente e in occasione di cambiamenti significativi che riguardano contesto, attività, servizi, requisiti applicabili o indirizzi strategici.

Revision #18

Created 2026-03-31 15:02:10 UTC by Davide Gelardi

Updated 2026-05-17 21:34:15 UTC by Davide Gelardi