



# SECURITY POLICY

Rev. 4 08/04/2026

Documento  
Riservato

Pagina 1 di 4

Elaborazione e Verifica

Amministratore di  
Sistema  
Aron Marinescu

Firma

.....

Approvazione ed Emissione

CEO  
Matteo Saltarello

Firma

.....

Data

08

04

2026

Data

08

04

2026

Rev	Causale (Emissione/Revisione)	Descrizione modifiche
01	Emissione	Prima emissione
02	Revisione	Classificazione del documento secondo la Procedura per la classificazione dei documenti rev.3
03	Revisione	Versione inglese
04	Revisione	Cambio logo e revisione testi

## SECURITY POLICY

La Direzione di Touch & Contact, consapevole dell'importanza e della necessità di avvalersi di un Sistema di Gestione per la Sicurezza delle Informazioni riconosciuto in ambito internazionale, al fine di garantire la qualità dei servizi forniti e perseguire la soddisfazione dei propri Clienti, ritiene opportuno rendere il proprio Sistema di Gestione Sicurezza delle Informazioni conforme allo standard ISO/IEC 27001:2022.

Obiettivi primari della presente politica di sicurezza delle informazioni aziendali sono i seguenti:

- Mettere a disposizione tutte le risorse necessarie al fine di rispettare i requisiti cogenti applicabili e assicurare nel tempo la conformità legislativa
- Impegnarsi per il miglioramento continuo del sistema di gestione ISO/IEC 27001:2022
- Tenere sotto controllo i fattori che emergono dalla valutazione dei rischi e avviare tutte le azioni possibili al fine della eliminazione o riduzione dei rischi
- Cogliere tutte le opportunità offerte dall'evoluzione della tecnologia, compatibilmente con le esigenze finanziarie dell'azienda, al fine di perseguire il miglioramento continuo del sistema di gestione
- Individuare con efficacia tutte le possibili minacce e vulnerabilità per eliminare o ridurre gli incidenti che da esse possono derivare
- Tenere sotto controllo i servizi in cloud da cui dipende la continuità del business aziendale
- Simulare incidenti per la sicurezza delle informazioni, al fine di verificare la capacità di reazione in termini di tempestività ed efficacia

- Attuare tutte le azioni possibili al fine di preservare l'integrità, la disponibilità e la riservatezza di qualunque asset appartenente a Touch & Contact;

Al fine di perseguire i citati obiettivi primari, si riportano di seguito alcuni esempi di interventi che la direzione promuove in azienda:

- Assegnare la responsabilità di tenuta sotto controllo degli asset aziendali al personale in modo che tutti, nelle modalità pertinenti al proprio ruolo e funzione, siano coinvolti e partecipi nella difesa del patrimonio delle informazioni di Touch & Contact;
- Stabilire modalità di controllo per il trasferimento all'esterno di asset aziendali;
- Assicurare che nell'alienazione di qualunque asset aziendale non si verifichi perdita in termini di riservatezza delle informazioni eventualmente in esso contenute;
- Controllare gli accessi dei visitatori negli uffici aziendali e tutti gli accessi a qualsivoglia informazione aziendale effettuata dal Personale o da terzi a vario titolo;
- Verificare che tutte le postazioni di lavoro abbiano accesso protetto da password periodicamente modificate;
- Definire e testare periodicamente procedure di back-up efficaci;
- Stabilire con i clienti e con i fornitori responsabilità reciproche nella gestione della sicurezza delle informazioni;
- Verificare periodicamente l'efficacia del piano di business continuity e disaster recovery.



## SECURITY POLICY

Rev. 4 08/04/2026

**Documento  
Riservato**

**Pagina 4 di 4**

Tutto il Personale, i collaboratori, i fornitori, i visitatori, dovranno operare nel rispetto delle norme e delle procedure aziendali predisposte al fine di assicurare la gestione del business aziendale in conformità ai predetti principi.

La Direzione si augura di ottenere, a tutti i livelli, la massima collaborazione per il rispetto e la sistematica applicazione di tali linee di indirizzo generali.

Roma lì, 19/05/2023 - aggiornato il 08/04/2026