

QUESTIONARIO ASSUNTIVO PER L'ASSICURAZIONE DEI RISCHI CYBER (CYBER RISK)

IMPORTANTE: Le risposte fornite nel presente questionario costituiranno la base contrattuale per l'eventuale emissione della polizza ai sensi degli articoli del Codice Civile applicabili. Risposte inesatte o reticenti possono compromettere il diritto al risarcimento.

SEZIONE 1: INFORMAZIONI GENERALI SUL CONTRAENTE

CAMPO	DATI DEL PROPONENTE/CONTRAENTE
Denominazione Sociale / Ragione Sociale:	
Sede Legale / Operativa:	
Partita IVA / Codice Fiscale:	
Settore di Attività / Codice ATECO:	
Sito Web Aziendale (URL):	
Fatturato Annuo Lordo (Ultimo Bilancio):	€
Quota di Fatturato all'Estero (se presente):	% USA/Canada % Resto del Mondo
Numero Totale Dipendenti e Collaboratori:	

SEZIONE 2: ARCHITETTURA IT E MISURE DI SICUREZZA (UNDERWRITING)

1) Accessi e Autenticazione

L'Azienda impone l'adozione di credenziali personali uniche e password complesse (almeno 8-12 caratteri, simboli, numeri) con cambio periodico obbligatorio?

SI ☐ NO ☐

È attiva l'Autenticazione a Due Fattori (MFA / 2FA) per l'accesso alla posta elettronica aziendale, alla rete interna e ai software gestionali core?

SI ☐ NO ☐

In caso di Smart Working o connessioni da remoto, il personale utilizza esclusivamente reti cifrate e protette tramite VPN aziendale?

SI ☐ NO ☐

2) Protezione Endpoint e Gestione Vulnerabilità

Tutti i dispositivi connessi alla rete (Server, PC, Laptop) sono protetti da un software Antivirus / Antimalware / EDR centralizzato e aggiornato quotidianamente?

SI ☐ NO ☐

Esiste una procedura standardizzata per l'installazione delle patch di sicurezza (aggiornamenti di sistema) entro 30 giorni dal loro rilascio?

SI ☐ NO ☐

L'Azienda utilizza sistemi operativi o software obsoleti non più supportati ufficialmente dai produttori (es. Windows 7, Windows Server 2008)?

SI ☐ NO ☐ (Se SÌ, specificare quali: _____)

3) Politiche di Backup e Resilienza (Business Continuity)

I backup dei dati aziendali, dei database clienti e dei software gestionali vengono eseguiti regolarmente con frequenza almeno giornaliera?

SI ☐ NO ☐

Esiste almeno una copia di backup conservata in modalità cifrata e strutturalmente isolata dalla rete principale (Offline, Immutabile o Cloud con accessi separati)?

SI ☐ NO ☐

Vengono effettuati test periodici (almeno una volta all'anno) per verificare l'effettiva leggibilità e la velocità di ripristino dei dati dai backup?

SI ☐ NO ☐

SEZIONE 3: GESTIONE DEI DATI, PRIVACY E FORMAZIONE (COMPLIANCE)

L'Azienda tratta o conserva dati sensibili, dati sanitari, dati giudiziari o numeri di carte di credito/conti correnti dei propri clienti?

SI ☐ NO ☐ (Se SÌ, specificare quali: _____)

È stata implementata una policy aziendale scritta (Regolamento Informatico) firmata dai dipendenti sull'uso corretto di internet, email e dispositivi?

SI ☐ NO ☐

I dipendenti e i collaboratori aziendali partecipano a sessioni periodiche di formazione o sensibilizzazione sui rischi Cyber (es. come riconoscere il Phishing)?

SI ☐ NO ☐

SEZIONE 4: DICHIARAZIONE SINISTRI PREGRESSI E CIRCOSTANZE NOTE

Negli ultimi 3 anni, la Società ha subito incidenti informatici, attacchi ransomware, violazioni di dati (data breach), frodi finanziarie digitali (phishing/social engineering) o blocchi operativi significativi?

SI ☐ NO ☐ (Se SÌ, specificare quali: _____)

Il Proponente è a conoscenza di fatti, circostanze, reclami scritti o contestazioni legali in corso che potrebbero dare origine a una richiesta di risarcimento coperta da questa polizza?

SI ☐ NO ☐

SEZIONE 5: FIRMA E CONSENSO ALLA VALUTAZIONE DEL RISCHIO

Il sottoscritto, in qualità di Legale Rappresentante dell'Azienda Proponente, dichiara che tutte le informazioni fornite in questo questionario sono esatte, complete e fedeli allo stato attuale dell'infrastruttura IT aziendale. Prende atto che il presente modulo non costituisce la conclusione del contratto assicurativo, ma la base tecnica essenziale per l'elaborazione della quotazione.

Luogo e data

Timbro dell'Azienda e Firma del Legale Rappresentante
