

Questo documento permette di raccogliere le informazioni necessarie per valutare i rischi connessi ai sistemi informativi dell'ente da assicurare. Si prega di notare che il completamento di questo questionario non vincola la compagnia destinataria né l'ente alla conclusione di un accordo per l'emissione di una polizza.

1. Identificazione dell'ente richiedente

Ragione sociale: *CORUNE DI SETTIMO MILANESE*

Indirizzo: *PIAZZA DEGLI EROI 5 - 20019 SETTIMO MILANESE*

Codice Fiscale/Partita IVA: *01315110150*

Sito/i Web: *WWW.CORUNE.SETTIMO.MILAN.ITALY*

Numero di dipendenti: *91*

Numero di transazioni derivanti da carte di pagamento (se applicabile):

Numero di abitanti: *20.094 (AL 31/12/2018)*

Totale componenti positivi della gestione (o totale entrate) presente su ultimo bilancio:

2. Profilo dell'ente da assicurare

Si prega di fornire l'elenco delle società controllate o partecipate con descrizione dell'attività e indicazione di fatturato.

Nome	Sede	Attività	Fatturato
<i>CORUNE SETTIMO M.</i>	<i>SETTIMO MIL.</i>	<i>ENTE LOCALE</i>	

3. Dichiarazioni

L'Ente dichiara:

Conferma:

1. Di non essere già assicurato, direttamente o tramite società controllanti, da polizza Cyber
2. Di non essere una società né di controllare società che operino nei seguenti settori: Istituzioni finanziarie (es: banche, SGR, SIM, Compagnie Assicurative, Asset manager)
3. Che tutti i dispositivi connessi alla rete sono protetti da firewall e sono dotati di software antivirus
4. Che il back up dei files viene effettuato almeno una volta al mese ed archiviato presso una sede separata
5. Che l'accesso alla rete aziendale e ai sistemi critici è protetto da password e viene implementata una politica inerente il controllo degli accessi
6. Che l'aggiornamento dei software e la verifica delle patch è effettuata almeno ogni 6 mesi.
7. Di non fornire servizi IT critici ad aziende terze o individui.
8. Di operare nel rispetto della normativa sulla Privacy e sul trattamento dei dati personali.
9. Di essere compliant con gli standard PCI-DSS (Payment Card Industry – Data Security Standards)
10. Di non essere a conoscenza di un qualunque incidente relativo alla sicurezza informatica o alla privacy verificatosi nei precedenti 36 mesi. Gli incidenti includono qualunque accesso non autorizzato a qualunque computer, sistema informatico, database, intrusione o attacco, impossibilità d'utilizzo di qualunque computer o sistema, interruzione premeditata, corruzione, o distruzione di dati, programmi, o applicazioni, qualunque evento di cyber estorsione; o qualunque altro incidente simile ai precedenti, inclusi quelli che hanno generato una richiesta di risarcimento, azione amministrativa, o procedimento da parte di un'autorità di vigilanza.

Il sottoscritto certifica che tutte le dichiarazioni contenute nel presente questionario sono complete e corrette. Tutte le modifiche che avvengono dopo la presentazione del questionario o durante il periodo di assicurazione devono essere comunicate alla Compagnia, immediatamente.

EMANUELA RADICE

Nome e Cognome del firmatario

COORDINATORE DIP. FINANZIARIO

Ruolo

Il Coordinatore del Dipartimento

Finanziario

Dott.ssa Emanuela Radice

Data

