MARSH

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

LEADERSHIP, KNOWLDGE, SOLUTIONS…WORDLWIDE.

MARSH & McLENNAN COMPANIES

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

polizza prestata nella forma " claims made" ed è soggetta alle relative condizioni. Questa polizza è valida solo in seguito alla richiesta di risarcimento da parte degli assicurati, segnalata per iscritto agli assicuratori entro il termine della polizza o dell'eventuale periodo di osservazione, se applicabile. I costi sostenuti come rimborso spese possono ridurre ed esaurire il limite di responsabilità e sono soggetti a franchigia.

Sezione 1. Informazioni generali sulla Proponente

1.1 Proponente

Nominativo: Comune di Reggio Emilia

Indirizzo: Piazza Prampolini 1

Reggio Emilia RE

Numero di Dipendenti: 1.376 al 31/12/2016 (dip. a tempo indeterminato)

1.2 Si prega di indicare:

Numero di cittadini serviti: 170.000

Importo retribuzioni: **32.807.430,25 (al 31/12/2016)**

Sezione 2. Carte di Pagamento

2.1 La proponente accetta pagamenti con carta di credito per beni o servizi? SI☒ NO

Se si:

2.1.1 Indicare la percentuale dei ricavi da transazioni con carta di credito negli ultimi dodici (12) mesi: i pagamenti con carta sono circa il 7% dei ricavi ottenuti tramite servizi on line.

Sezione 3. Gestione delle esposizioni della privacy

3.1 La Proponente è in possesso di una policy sulla privacy a livello aziendale? SI☒ NO☐

Limitamente al trattamento dei dati personali

3.2 La Proponente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali? **Il regolamento prevede che l'utilizzo di tutti gli strumenti informatici sia limitato all'attività lavorativa** SI☒ NO☐

3.3 Indicare quale tipo di informazioni sono registrate nel database:

Tipologia	Barrare se registrate	
Informazioni su carte di credito/debito	☐	
Informazioni sanitarie	☒	
Carta di identità	☒	Tutti i cittadini
Informazioni sulla previdenza (es. INPS)	☒	
Informazioni riguardo conti corrente	☒	dipendenti e fornitori dell'Ente
Proprietà Intellettuali del cliente	☐	
Altro *(specificare sotto)*	☐	Fare clic qui per immettere testo.

Sezione 4. Controlli dei sistemi informatici

4.1 La Proponente fornisce corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? SI☒ NO☐

4.2 La Proponente dispone di un:

Piano di disaster recovery	SI☐	NO☒
Piano di risposta alle intrusioni di rete e infezioni da virus	SI☐	NO☒

4.3 La Proponente sospende tutti gli accessi si computer e agli account quando un dipendente lascia l'azienda?	SI☒ NO☐

4.4 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della proponente :

Anti virus	☒
Firewall	☒
Rilevatori di intrusione	☒

4.5 Indicare se i laptop siano o meno protetti da firewall personali e/o i laptop possano connettersi solo tramite la rete aziendale si precisa che sui laptop viene installato antivirus, antispyware, antimalaware configurato per la gestione centralizzata (e quindi non disattivabile ne' modificabile dall'utente) e impostato per bloccare qualsiasi collegamento se non viene aggiornato collegandolo al server dell'ente. Inoltre l'utente non è amministratore del portatile e non puo' installare sw o cambiare la configurazione del sistema operativo	SI☐ NO☒
4.6 La Proponente dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni?	SI☒ NO☐
4.7 La Proponente possiede e applica una regolamentazione in materia di crittografia della comunicazione interna ed esterna?	SI☐ NO☒
4.8 La proponente impone un processo di aggiornamento dei software che includa l'installazione delle relative patch? Se si: 4.8.1 Le patch critiche sono installate entro 30 giorni dal rilascio?	SI☒ NO☐ SI☒ NO☐

Sezione 5. Fornitori e Terze Parti

5.1 La proponente esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete? SI☒ NO☐

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

Processo dei pagamenti	☐
IT Security	☐
Raccolta dati e/o processo	☐
Call center / Service desk	☒
Operational business process	☐
Altro *(specificare sotto)*	☐

I servizi di callcenter/ service desk vengono erogati da personali di una ditta esterna che opera presso la sede dell'ente. I pagamenti sono affidati al servizio di tesoreria esterno all'ente

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	☒
Esternalizzati in Host	☐
Esternalizzati in Cloud	☒

Non è un cloud pubblico ma sono servizi erogati dal datacenter di lepida società in house della regione ER

5.2 La Proponente esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate? SI☐ NO☒

Quando le sw house richiedono l'accesso ai sistemi dell'ente dall'esterno devono firmare una liberatoria in cui si impegnano ad attivare politiche di sicurezza adeguate

5.3 La proponente richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi? SI☐ NO☐

Quando le sw house richiedono l'accesso ai sistemi dell'ente dall'esterno devono firmare una liberatoria in cui si impegnano ad utilizzare i dati a cui hanno accesso solo per le manutenzioni dei sw stessi e a non diffonderli senza il consenso dell'ente

5.4 Indicare se la Proponente permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT SI☒ NO☐

Sezione 6. Contenuti multimediali, Website e Social Network

6.1 La proponente dispone di una procedura di risposta ad eventuali accuse che considerino il materiale creato, esposto o pubblicato dalla Proponente come diffamatorio, illegale o in violazione del diritto alla privacy di terzi? SI☐ NO☒

Sezione 7. Sinistri e circostanze

7.1 La Proponente è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della Proponente nei tre anni precedenti a questa richiesta? SI☐ NO☒

Se si, si prega di fornire dettagli di ciascun reclamo, accusa o episodio, includendo costi, perdite o danni subiti o pagati, e gli importi pagati come perdita sotto qualsiasi polizza assicurativa: Fare clic qui per immettere testo.

7.2 La Proponente ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza), attacchi DDoS ai propri sistemi informatici o tentativi di estorsione del proprio sistema informatico nei tre anni precedenti a questa richiesta o? SI☐ NO☒

Se si, si prega di descrivere le intrusioni o attacchi, compresi eventuali danni causati da tali intrusioni, fornendo indicazioni su tempo perso, ricavi persi, spese per riparare i danni ai sistemi o per ricostruire i database o i software: Fare clic qui per immettere testo.

7.3 La Proponente, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.
