**QUESTIONARIO CYBER RISK**

**IDENTIFICAZIONE DELL’ENTE E DELLE EVENTUALI SOCIETÀ CONTROLLATE**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. Denominazione dell’Ente contraente: | | | COMUNE DI CARONNO PERTUSELLA | | |
| 1. Indirizzo, CAP, Città: | | | PIAZZA ALDO MORO, 1 – 21042 CARONNO PERTUSELLA (VA) | | |
| 1. Codice Fiscale: | | | 00440710127 | | |
| 1. Partita IVA: | | | 00440710127 | | |
| 1. Numero di dipendenti: | | |  | | |
| 1. Numero di abitanti: | | |  | | |
| 1. Totale componenti positivi della gestione (voce del rendiconto della gestione dell’Ente): | | |  | | |
| 1. Numero di transazioni derivanti da carte di pagamento (se applicabile): | | |  | | |
| 1. Attività dell’Ente: | | |  | | |
| 1. Elenco delle società controllate da assicurare, descrizione dell’attività e indicazione di fatturato: | | | | | |
| Nome | Sede | | Attività | Fatturato |
|  |  | |  |  |
|  |  | |  |  |
|  |  | |  |  |
|  |  | |  |  |

**DICHIARAZIONI**

|  |  |  |
| --- | --- | --- |
| 1. Tutti i dispositivi connessi alla rete sono protetti da firewall e sono dotati di software antivirus? | SI | NO |
| 1. Il back up dei file viene effettuato almeno una volta al mese ed archiviato presso una sede separata? | SI | NO |
| 1. L’accesso alla rete aziendale e ai sistemi critici è protetto da password e viene implementata una politica inerente il controllo degli accessi? | SI | NO |
| 1. L’aggiornamento dei software e la verifica delle patch è effettuata almeno ogni 6 mesi? | SI | NO |
| 1. La Contraente fornisce servizi IT critici ad aziende terze o individui? | SI | NO |
| 1. La Contraente conferma che le politiche inerenti la protezione dei dati personali e la tutela della privacy sono periodicamente riviste al fine di essere allineate alle normative vigenti? | SI | NO |
| 1. La contraente dichiara che non si è mai verificato un qualunque incidente relativo alla sicurezza informatica o alla privacy 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 | SI | NO |
| 1. La Contraente è già assicurata, direttamente o tramite società controllanti, da polizza Cyber? | SI | NO |
| 1. Negli ultimi 3 anni ha avuto sinistri in ambito di sicurezza informatica o privacy? | SI | NO |
| 1. La Contraente opera direttamente o ha Controllate che operano in uno dei seguenti settori?    * Istituzioni finanziarie (es: banche, SGR, SIM, Compagnie Assicurative, Asset manager)   • Gestori di infrastrutture critiche, incluse Utility ed Energia  • Centro scommesse/Centro scommesse sportive | SI | NO |
| 1. La Contraente, o il provider a cui è affidato il servizio, accetta pagamento con carte di credito/debito? | SI | NO |

|  |  |  |
| --- | --- | --- |
| Data  6 febbraio 2023 |  | Firma |