

Chubb Easy Solutions

Cyber Enterprise Risk Management 2.2 - Enti Comunali

Ed. 10/2022

Proposta di Rinnovo Nr: RITCYN004552

Data Emissione: 02/04/2025

Data Scadenza: 02/05/2025

CHUBB®

Servizi informatici Chubb

**Colmare il divario tra assicurazioni Cyber e competenze in materia di sicurezza informatica**

Con una polizza cyber di Chubb, non solo ricevete una protezione finanziaria dai costi e dalle responsabilità conseguenti a una violazione dei dati, a un attacco informatico e a un'interruzione di sistema, ma supportiamo anche gli assicurati nella gestione, nella preparazione e nella prevenzione degli incidenti attraverso i nostri servizi e la nostra consulenza informatica. I servizi, progettati per affrontare le minacce informatiche più comuni e ridurre le esposizioni, sono disponibili per tutti gli assicurati cyber di Chubb. Per saperne di più o per richiedere i servizi informatici, visitate il sito www.chubb.com/it-it/servizi-cyber-italia.html.

Soluzione e Servizi		Gratuito	Scontato
Soluzioni di gestione delle vulnerabilità informatiche – per essere sempre al corrente delle vulnerabilità del software e della rete			
Programma di sensibilizzazione sulle vulnerabilità	Iscrivetevi per ricevere avvisi di emergenza e consigli pratici sulla mitigazione delle nuove vulnerabilità critiche che vengono sfruttate, personalizzati in base al software che utilizzate.	☑	
Supply Chain Risk Management	Mitiga la vulnerabilità e le minacce all'interno della tua supply chain, proteggendo le tue attività aziendali da possibili compromissioni da parte di fornitori o partner commerciali	☑	
Monitoraggio delle vulnerabilità esterne	Monitorare il rischio informatico come misura quotidiana delle prestazioni di sicurezza attraverso una piattaforma che evidenzia sia i punti di forza che i potenziali punti deboli, fornendo metriche chiave e visibilità sulla sicurezza dell'organizzazione.	☑	
Preparazione, Formazione e Servizi di Risposta			
Cyber Alert App	L'App Cyber Alert offre la segnalazione degli incidenti 24 ore su 24, 7 giorni su 7, da un dispositivo mobile o da un computer e consente ai clienti di pre-registrare i dettagli di contatto e le informazioni sulla polizza per una gestione efficiente della risposta agli incidenti.	☑	
Endpoint Security & Response	Ottenete l'accesso a un software antivirus di ultima generazione che fornisce un rilevamento 24 ore su 24 e protegge i punti di ingresso vulnerabili della vostra rete da molte minacce ransomware.		☑
Password Management Application	Protegete e gestite le password degli utenti con una soluzione che ricorda e compila automaticamente password, login, informazioni personali e dettagli di pagamento, incoraggiando un uso responsabile delle password.	☑	
Phishing Awareness Training	Distribuite ai vostri dipendenti scenari di phishing simulati e reali, accompagnati da una formazione per gli utenti e da un rapporto sui risultati con raccomandazioni per il miglioramento del rischio.		☑

Ottenete il massimo valore dalla vostra polizza Chubb e richiedete i servizi informatici visitando il sito www.chubb.com/it-it/servizi-cyber-italia.html

Chubb Easy Solutions

Cyber Enterprise Risk Management 2.2 - Enti Comunali

Ed. 10/2022

SCHEDA DI POLIZZA

1	Contraente	COMUNE DI CUORGNE'
	Indirizzo	VIA GIUSEPPE GARIBALDI 9 - CUORGNE' - 10082 (TO)
	Codice Fiscale/P.IVA	02180640019
2	Periodo Assicurativo	Effetto: dalle ore 24:00 del 30/06/2025 Scadenza: alle ore 24:00 del 30/06/2026

Opzione Nr. 1					
3	Limite Aggregato di Polizza		€ 500.000		
	Garanzie Danni Propri (Limite)		con riferimento a un:	per Periodo Assicurativo	Franchigia per Sinistro
	1.1	Spese di Incident Response	Fornitori Preferiti Chubb	€ 500.000	€ 0
			Fornitori Non Preferiti	€ 500.000	€ 10.000
	1.2	Perdite per Interruzione dell'Attività Aziendale	Sistema Informatico Assicurato	€ 500.000	€ 10.000
			Sistema Informatico Condiviso	€ 500.000	Periodo di Carenza: 12 ore
					€ 10.000
					Periodo di Carenza: 12 ore
	1.3	Costi di Recupero di Dati e Sistemi	Sistema Informatico Assicurato	€ 500.000	€ 10.000
			Sistema Informatico Condiviso	€ 500.000	€ 10.000
	1.4	Perdite per Cyber Estorsione	Sistema Informatico Assicurato	€ 500.000	€ 10.000
			Sistema Informatico Condiviso	€ 500.000	€ 10.000
	Garanzie Responsabilità Civile verso Terzi (Limite)			per Periodo Assicurativo	Franchigia per Sinistro
	1.5	Responsabilità Violazione Privacy e Sicurezza Rete		€ 500.000	€ 10.000
	1.6	Responsabilità Derivante dai Media		€ 500.000	€ 10.000
	Estensioni Copertura (Limite)		con riferimento a un:	per Periodo Assicurativo	Franchigia per Sinistro
	2.1	Spese di Emergenza di Incident Response		€ 50.000	€ 0
	2.2	Costi di Miglioramento		€ 50.000	€ 10.000
	2.3	Crimine Informatico	Sistema Informatico Assicurato	€ 25.000	€ 10.000
			Sistema Informatico Condiviso	€ 25.000	€ 10.000
	2.4	Premio di Ricompensa		€ 50.000	€ 0
	2.5	Frodi Relative alle Telecomunicazioni	Sistema Informatico Assicurato	€ 25.000	€ 10.000
Sistema Informatico Condiviso			€ 25.000	€ 10.000	
Sottolimiti			per Periodo Assicurativo	Franchigia per Sinistro	

Fondo Ricorso Consumatori			€ 50.000	€ 10.000
Perdite Derivanti da Carte di Pagamento			NON OPERANTE	NON OPERANTE
Sanzioni dell'Organo di Vigilanza			€ 50.000	€ 10.000
Ulteriori Sottolimiti	Giorni	Scoperto Aggiuntivo	per Periodo Assicurativo	Franchigia
Ransomware		0 %	€ 500.000	€ 10.000
Perdite per Sfruttamento Software Trascurato	0 - 45	0%	100% del limite	Franchigia generale
	46 - 90	5%	50% del limite	Franchigia generale
	91 - 180	10%	25% del limite	Franchigia generale
	181 - 365	25%	10% del limite	Franchigia generale
	Oltre 365	50%	5% del limite	Franchigia generale
Sottolimiti per Eventi a Impatto Diffuso				
Sfruttamento Vulnerabilità Note			€ 50.000	€ 10.000
Sfruttamento Vulnerabilità nella Supply Chain di un Software			€ 50.000	€ 10.000
Sfruttamento Vulnerabilità Zero Day			€ 50.000	€ 10.000
Qualsiasi Altro Evento a Impatto Diffuso			€ 50.000	€ 10.000
4	Data di Retroattività	30/06/2020		
5	Periodo di Indennizzo	90 giorni		
6	Periodo di Garanzia Postuma	12 mesi con premio imponibile addizionale pari al 100% dell'ultimo premio imponibile annuo		
7	Intermediario	HOWDEN ASSITECA S.P.A. (ASSIO545)		
8	Premio	Rateo dal 30/06/2025 al 30/06/2026 (gg 360/360) di premio annuo € 3.743,15		
	Rate	Imponibile	Imposte	Lordo
	Opzione Nr. 1 - Limite 500.000			
	Alla Firma (30/06/2025)	€ 3.743,15	€ 829,58	€ 4.572,73
	Rate Successive dal 30/06/2026	€ 3.743,15	€ 829,58	€ 4.572,73

Milano 02/04/2025

INFORMAZIONI SUL RISCHIO (QUESTIONARIO)

Informazioni Generali		
Numero di Abitanti	9.612	
Nr. Dipendenti	//	
Totale componenti positive della gestione	€ 5.450.000	
La Società è già assicurata, direttamente o tramite Società Controllanti, da polizza Cyber in vigore con Chubb?	NO	
Sito web L'indirizzo del sito web fornito fa parte della dichiarazione e può avere un impatto sui termini e sulle condizioni.	comune.cuorgne.to.it	
Attività Svolta - Settore	ENTE COMUNALE	
Attività Svolta - NAIC	Uffici Direzionali - 921110	
Dati di contatto del Responsabile della sicurezza dei dati e della rete		
La Società acconsente che Chubb contatti eventualmente il responsabile IT nell'ambito della gestione del rischio?		NO
Nome e cognome	//	
Ruolo	//	
e-mail	//	
Telefono	//	
1	La Società fornisce servizi o ha rapporti commerciali con Individui e/o Organizzazioni in territori sanzionati (inclusi - a titolo esemplificativo ma non esaustivo, Iran, Siria, Nord Sudan, Crimea e Cuba) o qualsiasi altro territorio soggetto a sanzioni USA, UE, ONU e/o altre restrizioni nazionali?	NO
2	La Società ha sede in Italia ed è una controllata, filiale, franchisee o un'entità di un'organizzazione più grande? Se la Società è una filiale/controllata di un fondo di Prive Equity, selezionare "NO".	NO
3	La Società e/o le sue Controllate, operano in uno dei seguenti settori:	
	• Istituzioni finanziarie	[]
	• Aste online/Centro scommesse/Centro scommesse sportive/ Gioco d'azzardo	[]
	• Sviluppo Software e/o servizi IT ad aziende terze o individui	[]
	• Gestori di infrastrutture critiche, incluse Utility ed Energia	[]
	• Nessuna delle precedenti	[X]
4	In caso di violazione delle Informazioni di Identificazione Personale , la notifica da parte della Società potrebbe riguardare un numero maggiore di 500.000 individui?	<= 500.000
5	L'assicurato è conforme agli standard di Payment Card Industry Data Security Regulation (o PCI-DSS) ?	Pagamento con carte di Credito/Debito non consentito e nessuna raccolta di dati di carte di pagamento
6	Si è mai verificato un qualunque Incidente Cyber, Data Breach o reclamo in materia di privacy nei precedenti 3 anni, o si è al corrente di qualsiasi circostanza che possa dare origine ad un sinistro nell'ambito della polizza Cyber?	NO
6.1	Se sì, Si prega di indicare il numero e l'importo applicabile degli incidenti informatici assicurati o meno (compresi quelli al di sotto della franchigia).	
	Numero di Sinistri	//
	Importo totale pagato	//
7	La Contraente ha Società Controllate con sede in Paesi extra UE per le quali è richiesta la copertura assicurativa?	NO

8	Le politiche inerenti la protezione dei dati personali e la tutela della privacy sono periodicamente riviste al fine di essere allineate alle Normative Vigenti nelle giurisdizioni in cui opera?	SI
	L'assicurato dispone di un' autenticazione a più fattori (MFA) completamente implementata per l'accesso remoto ai diversi sistemi che la richiedono, compresa la posta elettronica?	<input checked="" type="checkbox"/> Sì <input type="checkbox"/> Sì, ma parzialmente implementata <input type="checkbox"/> No, ma verrà implementata entro 6 mesi <input type="checkbox"/> No <input type="checkbox"/> No, l'accesso da remoto non e' previsto
Selezionare le misure che la Società utilizza a protezione dei back up dei sistemi critici per l'attività aziendale		
	Immutable back up: i back up, una volta memorizzati su uno storage, non possono essere modificati (Write Once Read Many - WORM)	<input checked="" type="checkbox"/>
	I back up vengono archiviati offline o presso una ambiente/storage separato (es. nastro, dischi completamente disconnessi rispetto al resto della rete)	<input checked="" type="checkbox"/>
	l'accesso ai backup è limitato solo ad Account Privilegiati dedicati che non sono collegati all' Active Directory o ad altri domini	<input checked="" type="checkbox"/>
	l'accesso ai backup è protetto tramite l'autenticazione a più fattori MFA (Multi-Factor Authentication)	<input checked="" type="checkbox"/>
	Nessuna delle protezioni elencate precedenti	<input type="checkbox"/>
Selezionare quali tecnologie la Società utilizza a protezione degli endpoint su tutti i laptop, desktop e server		
	Sistemi di Advanced Endpoint Protection o in grado di effettuare Analisi di tipo Euristico	<input checked="" type="checkbox"/>
	Filtro URL o Web - filtering	<input checked="" type="checkbox"/>
	Tecnologie di isolamento e contenimento delle applicazioni	<input checked="" type="checkbox"/>
	Piattaforma centralizzata per la Endpoint Protection	<input checked="" type="checkbox"/>
	EDR (Endpoint Detection and Response), XDR (Extended Detection and Response), o MDR (Managed Detection and Response)	<input type="checkbox"/>
	Nessuna delle protezioni elencate precedenti	<input type="checkbox"/>
Selezionare quali misure la Società utilizza a protezione delle e-mail		
	Servizio di quarantena per e-mail sospette	<input checked="" type="checkbox"/>
	Disponibilità di Sandbox per la verifica di allegati potenzialmente sospetti	<input checked="" type="checkbox"/>
	Applicazione del Sender Policy Framework (SPF) .	<input checked="" type="checkbox"/>
	Le macro di Microsoft Office sono disabilitate sui documenti per impostazione predefinita	<input checked="" type="checkbox"/>
	Simulazioni di phishing o altra formazione per i dipendenti con cadenza almeno annuale	<input checked="" type="checkbox"/>
	Nessuna delle protezioni elencate precedenti	<input type="checkbox"/>

CONDIZIONI DI ASSICURAZIONE

Alla presente Proposta di Assicurazione si applicano le Condizioni di Assicurazione **Cyber Enterprise Risk Management 2.2 - Enti Comunali - Ed. 10/2022** contenute nel Set Informativo che forma parte integrante della presente Proposta.

CONDIZIONI PARICOLARI

Il **Contraente/Assicurato** dà atto che le seguenti Sezioni e Clausole Particolari non sono predisposte unilateralmente dall'**Assicuratore**, ma sono il risultato di una specifica trattativa tra le Parti contraenti, con conseguente inapplicabilità degli artt. 1341 e 1342 del Codice Civile.

1) SERVIZIO DI CYBER INCIDENT RESPONSE

Con la presente Condizione Particolare si conviene quanto segue:

*) SERVIZIO DI CYBER INCIDENT RESPONSE - FORNITORI PREFERITI CHUBB E CLAUSOLA DI EMERGENZA DI INCIDENT RESPONSE

Tale clausola offre servizi di gestione della crisi consentendo all'**Assicurato** di selezionare i fornitori in relazione alle coperture **Spese di Incident Response** o **Spese di Emergenza di Incident Response** prestate con le polizze Cyber Chubb.

In caso di un **Incidente informatico** o **Interruzione dell'Attività Aziendale**, l'**Assicurato** potrà contattare il **Chubb Cyber Incident Response Centre** attraverso una delle seguenti modalità:

App Chubb Cyber Alert: scaricabile per dispositivi iPhone e Android su www.chubbcyberalert.com

Sito web Chubb Cyber Alert: www.chubbcyberalert.com

Chubb Cyber Alert Hotline: 800 194 721

La sezione 3 della **Scheda di Polizza** è modificata eliminando la riga relativa alle **Spese di Incident Response** ed alle **Spese di Emergenza di Incident Response** e sostituendola come segue:

Garanzie Danni Propri : Spese di Incident response

- Fornitori Preferiti Chubb

Limite per Periodo Assicurativo : Full Limit

Franchigia per Sinistro : €0

- Fornitori Non Preferiti

Limite per Periodo Assicurativo : Full Limit

Franchigia per Sinistro : Come da **scheda di Polizza**

Estensione di Copertura : Spese di Emergenza di Incident Response

Limite per Periodo Assicurativo: € 50.000

Franchigia per Sinistro: €0

La sezione *Garanzie Base* è modificata eliminando la clausola Garanzie Danni Propri relativa alle Spese di Incident Response e sostituendola come segue: Spese di Incident Response

Le **Spese di Incident Response** sostenute mediante l'uso dei **Fornitori Preferiti Chubb** o **Fornitori Non Preferiti** in conseguenza di un **Incidente Informatico** o di un'**Interruzione dell'Attività Aziendale** scoperti per la prima volta da un membro del **Gruppo di Controllo** durante il **Periodo Assicurativo**. Tale **Incidente Informatico** o **Interruzione dell'Attività Aziendale** dovranno essere stati denunciati all'**Assicuratore** ai sensi dell'art. 5.8 "Denuncia dei Sinistri - Obblighi degli Assicurati";

L'**Assicurato** non ha alcun obbligo di utilizzare o stipulare contratti per i servizi con i **Fornitori Preferiti Chubb**. Tuttavia, il **Limite per Periodo Assicurativo** applicato e la **Franchigia per Sinistro** specificata nella **Scheda di Polizza** verranno applicate in base alla scelta dell'**Assicurato** di utilizzare o stipulare un contratto con qualsiasi **Fornitore Preferito Chubb** o **Fornitore Non Preferito**.

La sezione *Estensioni di Copertura* è modificata eliminando la clausola relativa alle Spese di Emergenza di Incident Response e sostituendola come segue: Spese di Emergenza di Incident Response

Le **Spese di Emergenza di Incident Response** sostenute mediante l'uso dei **Fornitori Preferiti Chubb** nelle prime 48 ore immediatamente successive alla scoperta da parte di un membro del **Gruppo di Controllo** per la prima volta durante il **Periodo Assicurativo** di un **Incidente Informatico** o un'**Interruzione dell'Attività Aziendale**, effettivi o ragionevolmente sospettati. Tali **Incidente Informatico** o **Interruzione dell'Attività Aziendale** dovranno essere stati denunciati all'**Assicuratore** ai sensi dell'art. 5.8 "Denuncia dei Sinistri - Obblighi degli Assicurati". La sezione 3 'Definizioni Generali di Polizza' è modificata aggiungendo le seguenti definizioni: **Chubb Cyber Incident Response Centre**: servizio di call center di emergenza con lo scopo di contattare i **Fornitori Preferiti Chubb**. **Fornitori Preferiti Chubb**: qualsiasi azienda o società designata o impegnata attraverso l'uso del **Chubb Cyber Incident Response Centre** per fornire servizi di risposta agli incidenti descritti nel testo di polizza cyber di Chubb.

Una lista dei **Fornitori Preferiti Chubb** è disponibile su richiesta.

Fornitori Non Preferiti: qualsiasi azienda che fornisca i servizi indicati nella definizione di **Spese di Incident Response** a un **Assicurato** che non sia un **Fornitore Preferito Chubb**. La sezione *Definizioni Generali di Polizza* è modificata eliminando la definizione **Spese di Emergenza di Incident Response** e sostituendola come segue[A1]:

Spese di Emergenza di Incident Response: (applicabile solo alla garanzia indicata al punto 2.1 dell'art. 2 "Oggetto dell'Assicurazione: Estensioni di Copertura") le spese ragionevoli e necessarie:

per avvalersi dei servizi di un gestore di servizi di cyber incident response assegnati contattando il **Chubb Cyber Incident Response Centre** al fine di coordinare la risposta in caso di un **Incidente informatico** o **Interruzione dell'Attività Aziendale**, effettivi o ragionevolmente sospettati, per avvalersi dei servizi di una società specializzata in informatica forense assegnati contattando il **Chubb Cyber Incident Response Centre** al fine di determinare la causa e la portata di un **Incidente Informatico** o di un **Interruzione dell'Attività Aziendale** dell'**Assicurato**, accertati o ragionevolmente sospettati, e per avviare il processo necessario per interrompere, invertire o porre rimedio agli effetti di tale **Incidente Informatico** o **Interruzione dell'Attività Aziendale**.

Le **Spese di Emergenza di Incident Response** sono da intendersi parte e non in aggiunta al **Limite per Periodo Assicurativo** riportato nella Scheda di Polizza per "Incident Response" ai sensi del punto 1.1 dell'art. 1 "Oggetto dell'Assicurazione: Garanzie Base", e lo riducono e possono completamente esaurirlo.

La sezione 5 'Condizioni Generali applicabili a tutte le Garanzie' è modificata aggiungendo quanto segue: L'art. 5.8 "Denuncia dei Sinistri - Obblighi degli Assicurati" è da intendersi integrato con il seguente paragrafo:

E. Se l' **Assicurato** contatta il **Chubb Cyber Incident Response Centre** per assistenza in caso di **Incidente Informatico** o di **Interruzione dell'Attività Aziendale**, l'**Assicurato** avrà a disposizione le seguenti due opzioni:

Opzione 1: Il **Chubb Cyber Incident Response Centre** provvederà ad informare l'**Assicuratore** per conto dell'**Assicurato**.

L'**Assicurato** può scegliere di fare in modo che il **Chubb Cyber Incident Response Centre** fornisca notifica per suo conto all'**Assicuratore**. Al fine di esercitare tale opzione, l'**Assicurato** deve dare esplicito consenso al **Chubb Cyber Incident Response Centre** per consentire loro di fornire notifica all'**Assicuratore** per conto dell'**Assicurato**. I requisiti di notifica dell'**Assicurato** sono soddisfatti se l'**Assicurato** fornisce consenso specifico al **Chubb Cyber Incident Response Centre** al fine di eseguire tale attività per conto dell'**Assicurato**.

Opzione 2: Il **Chubb Cyber Incident Response Center** non provvederà ad informare l'**Assicuratore** per conto dell'**Assicurato**.

L'**Assicurato** non è obbligato a dare il suo consenso al **Chubb Cyber Incident Response Centre** per fornire notifica all'**Assicuratore** in caso di un **Incidente Informatico** o di un **Interruzione dell'Attività Aziendale**, anche se l'**Assicurato** sceglie di utilizzare i suoi servizi. Se l'**Assicurato** decide di non consentire al **Chubb Cyber Incident Response Centre** di fornire notifica per suo conto, allora l'**Assicurato** deve notificarlo all'**Assicuratore** come indicato nell'art 5.8 "Denuncia dei Sinistri - Obblighi degli Assicurati".

Si richiama infine l'attenzione del **Contraente** su quanto segue:

L'**Assicurato** non è tenuto a sottoscrivere un contratto per la fornitura dei servizi con i **Fornitori Preferiti Chubb** o i **Fornitori Non Preferiti**. L'**Assicuratore** non è in alcun modo tenuto a fornire qualsiasi servizio previsto nel contratto di fornitura con i **Fornitori Preferiti Chubb** o i **Fornitori Non Preferiti**. I **Fornitori Preferiti Chubb** ed i **Fornitori Non Preferiti** sono soggetti esterni all'**Assicuratore** e non sono suoi agenti o

rappresentanti. L'**Assicurato** accetta che l'**Assicuratore** non si assumerà alcuna responsabilità derivante da qualunque servizio reso da qualsiasi fornitore esterno del servizio. L'**Assicuratore** non sarà titolare di alcun diritto né di alcuna obbligazione o responsabilità eventualmente stabilita in qualsiasi accordo stipulato tra l'**Assicurato** e qualsiasi fornitore di servizi terzi. L'**Assicurato** prende atto che i servizi per cui stipula il contratto possono comprendere servizi parzialmente o totalmente non coperti dalla presente **Polizza** e, in tal senso, in questa, l'**Assicuratore** non ha alcun obbligo di notifica nei confronti dell'**Assicurato**. Qualunque diritto od obbligazione in relazione a tali accordi, comprese fatturazioni, compensi e servizi resi associati all'utilizzo dei **Fornitori Preferiti Chubb** e **Fornitori Non Preferiti** saranno in capo all'**Assicurato** quando tali servizi sono parzialmente o totalmente non coperti dalla presente **Polizza**.

Fermo il Resto

2) PRECISAZIONE CODICE CIG

Si precisa che il Codice CIG è: B221659760

Servizi di Loss Mitigation disponibili per i nostri Assicurati

Chubb vuole impegnarsi aiutando i suoi Clienti a migliorare le politiche di cyber risk management. Abbiamo stabilito diverse partnership con aziende specializzate in servizi di cyber security con l'obiettivo di offrire servizi di loss mitigation ai nostri Assicurati.

Di seguito i dettagli relativi a tali servizi, previsti per rispondere alle comuni minacce in ambito cyber. Visitate <http://www.chubb.com/cyber-services> ulteriori informazioni.

Cyber Alert App <i>fornita da Chubb</i>	Cyber Alert App offre un servizio attivo 24/7 per la notifica dell'incidente attraverso smartphone o computer e permette ai clienti di registrare preventivamente i riferimenti di polizza e i contatti utili ad una gestione efficiente delle attività di incident response.
	Costo aggiuntivo: gratuito - download disponibile per dispositivi iPhone e Android
Personal Cyber Risk Dashboard <i>fornita da DynaRisk</i>	Personal Cyber Risk Dashboard offre servizi di assessment del proprio rischio online, scansioni di dispositivi per vulnerabilità e data breach, e un piano d'azione con raccomandazioni su come migliorare il proprio profilo di rischio online. La dashboard, inoltre, invia alerts relativi alle minacce più rilevanti agli utenti.
	Costo aggiuntivo: gratuito - cinque licenze individuali disponibili gratuitamente ai titolari di polizze Cyber ERM.
Password Management Application <i>fornita da Dashlane</i>	L'applicazione Password Management permette di gestire e proteggere le password degli utenti, fornendo un servizio di completamento automatico di credenziali di login, informazioni personali e informazioni per effettuare pagamenti al fine di incoraggiare un utilizzo responsabile delle password. Dashlane comprende anche un servizio di monitoraggio del Dark Web e di notifica delle minacce principali.
	Costo aggiuntivo: gratuito - 500 licenze individuali sono disponibili per i nostri assicurati
Phishing Awareness Training <i>fornita da Cofense</i>	Phishing Awareness Training include due simulazioni di scenari reali di phishing nel corso di 4 mesi e per un massimo di 500 dipendenti. Al termine del programma, i risultati saranno riepilogati in un report che includerà il riepilogo dell'attività svolta, un'analisi dettagliata del grado di vulnerabilità generale, il tasso di eventi da segnalare, il tasso di recidiva e molto altro. Il consulente Cofense fornirà inoltre osservazioni e raccomandazioni su come proseguire con il programma.
	Costo aggiuntivo: € 2.400 - in aggiunta al premio di polizza
Per ulteriori informazioni su come accedere ai servizi di Loss Mitigation si prega di visitare http://www.chubb.com/cyber-services	

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi della vigente normativa nel quadro del Regolamento UE 2016/679 (Regolamento Generale in materia di Dati Personali), noi di Chubb European Group SE - Sede Secondaria e Direzione Generale della Società in Italia - Via Fabio Filzi, 29 - 20124 Milano - Titolare del trattamento - trattiamo i dati personali forniti dal contraente o raccolti tramite soggetti da noi autorizzati, come per esempio gli intermediari assicurativi, per le finalità connesse alla sottoscrizione e gestione delle polizze nonché per la valutazione di eventuali richieste di indennizzo derivanti dal verificarsi di un sinistro.

I dati che potranno essere da noi trattati sono dati personali identificativi e di recapito, quali ad esempio nome, cognome, indirizzo, numero di polizza, dati che riguardano controversie civili o condanne penali e reati così come, previo consenso dell'interessato, particolari categorie di dati quali - per esempio - i dati inerenti allo stato di salute dell'interessato stesso (di seguito tutti insieme i "Dati") nell'ipotesi in cui ciò sia necessario al fine di valutare l'entità del sinistro, definire il livello di rischio assicurativo ed in generale adempiere ad ogni specifica richiesta.

Inoltre nel caso venga richiesto lo specifico consenso espresso dell'interessato, i dati potranno essere utilizzati per contattarlo con strumenti tradizionali (per posta e tramite telefono e con l'ausilio di un operatore) ed automatizzati (per posta elettronica, sms, mms, fax e social media) per inviargli offerte sui nostri prodotti. Resta inteso che in ogni momento l'interessato potrà revocare tale consenso o limitarlo anche ad uno solo dei suddetti canali di comunicazione. Precisiamo che tale ultima finalità verrà perseguita solo nel caso sia richiesto ed ottenuto il consenso a tale trattamento.

Per lo svolgimento delle sole finalità amministrative e contrattuali, i Suoi Dati potranno essere comunicati alle altre società del Gruppo anche ubicate all'estero. Al fine di adempiere alle richieste derivanti dalla gestione della polizza, ci avvaliamo anche di soggetti terzi autorizzati al trattamento dei Suoi Dati che operano secondo e nei limiti delle istruzioni da noi impartite.

I dati saranno conservati per il tempo strettamente necessario alla gestione delle finalità sopra descritte.

L'interessato ha diritto di accedere ai Dati in ogni momento, opporsi al trattamento dei medesimi, chiederne la rettifica, la modifica e/o cancellazione ed esercitare il diritto alla limitazione dei trattamenti e il diritto alla portabilità dei dati. A tale fine può rivolgersi a Chubb European Group SE - Rappresentanza Generale per l'Italia - Via Fabio Filzi, 29 - 20124 Milano (MI) - Tel. 02-270951- Fax: 02-27095333 o contattare il Responsabile per la Protezione dei Dati Personali all'indirizzo dataprotectionoffice.europe@chubb.com. Da ultimo, si ricorda che ogni interessato ha diritto di proporre reclamo all'Autorità Garante in materia di Protezione dei Dati Personali.

L'Informativa completa sul trattamento dei Dati da parte di Chubb, con l'indicazione dettagliata delle basi giuridiche del trattamento è disponibile sul nostro sito internet www.chubb.com/it o direttamente al seguente link <https://www2.chubb.com/it-it/footer/privacy-statement.aspx>. È altresì possibile richiedere una copia cartacea dell'Informativa completa in ogni momento, inviando una email a: dataprotectionoffice.europe@chubb.com.