Questionario Polizza Cyber Risk – Enti pubblici

LEGENDA

Ai fini della compilazione del questionario vi riportiamo di seguito alcune indicazioni:
1) **domande bianche o non evidenziate con nessun colore**: sono domande per lo più identificative dell'Ente e riguardanti la sua situazione (es. numero di abitanti, eventuali sinistri cyber, presenza di società controllate da inserire nel perimetro assicurato, mappatura asset presenti).
2) **domande evidenziate in** sono domande estremamente importanti che indagano la presenza di misure tecniche ed organizzative di cui l'Ente deve essere in possesso per poter essere assicurato.
3) **domande evidenziate in** sono domande importanti che indagano la presenza di misure tecniche ed organizzative e che possono avere un impatto sul normativo, sui deducibili e sul premio.
3) **domande evidenziate in** sono domande meno rilevanti rispetto alle precedenti che indagano la presenza di misure tecniche ed organizzative e che possono avere un impatto minore sul normativo, sui deducibili e sul premio.

Sez.1
DATI GENERALI E SITUAZIONE ENTE

DATI GENERALI

Denominazione Ente	Comune di Calcio
Cod. Fiscale / Partita IVA	00372530162
Indirizzo	Via Papa Giovanni XXIII, 40 - 24054 Calcio (BG)
Numero abitanti	Al 31.12.2023: n. 5484
Numero dipendenti	17 (oltre al Segretario Generale)
Indirizzo web	https://www.comune.calcio.bg.it/it
Accettati pagamenti con carta di credito per beni e servizi	☐si ☒ no

SOCIETA' CONTROLLATE

Nome	Sede	Attività	Fatturato (Mln/€)
Per elenco partecipazioni del comune vedere: - https://shorturl.at/aCDIS - https://shorturl.at/eMRY0 - https://shorturl.at/dxEUX - https://shorturl.at/bivAR			

SITUAZIONE SINISTRI		
	Sinistri accaduti negli ultimi 3 anni ai sensi della polizza Cyber	☐ si ☒ no
	In caso affermativo, la violazione ha riguardato: **SI CHIEDE INOLTRE DI COMPILARE L'ALLEGATO 2**	☐Violazione della privacy, divulgazione non autorizzata o perdita di informazioni riservate ☐ Reclami/Segnalazioni da parte degli interessati ☐ Violazione del sistema informatico (attacchi informatici, intrusioni, violazioni della rete o simili) ☐ Interruzione di servizio non programmata
	L'organizzazione ha subìto dei controlli e delle visite ispettive in materia privacy da parte dell'Autorità?	☐ si ☒no In caso affermativo, indicare l'esito dell'ispezione: _____

MAPPATURA DEGLI ASSET AZIENDALI		
	Indicare il numero dei computer fissi	☒ <100 ☐ 101-1000 ☐ >1001
	Indicare il numero dei device mobili utilizzati:	Tablet ☒ <100 ☐ 101-1000 ☐ >1001 Smartphone ☒ <100 ☐ 101-1000 ☐ >1001 Laptop ☒ <100 ☐ 101-1000 ☐ >1001
	Indicare i sistemi operativi utilizzati sui client fissi/laptop	☐ precedenti a Windows 10 ☒Windows 10 ☐Mac ☐Linux ☒ Altro, specificare Windows 11
	Indicare i sistemi operativi utilizzati su tablet/smartphone	☒ Android ☐IOS
	Indicare il numero dei server	☒ <10 ☐ <100 ☐ 101-1000 ☐ >1001
	Indicare le modalità di gestione dei data center	☒ in house (i file e le cartelle condivise su cui i dipendenti lavorano) ☐esternalizzati in hosting/housing ☒ in cloud (i database)
	Indicare i sistemi operativi utilizzati sui server	☐precedenti o pari a Windows Server 2008 R2 ☒ Windows Server 2016 o superiore ☐Linux ☐ Altro, specificare
	Nel caso in cui l'Organizzazione utilizzasse dei sistemi o software non più supportati dal produttore:	
	Fornire lista software/hardware end-of-life e relativo piano di dismissione e/o ragione dietro l'assenza di un piano di dismissione.	Non presenti
	Indicare in quali processi sono coinvolti i sistemi legacy	Non presenti
	L'organizzazione ha acquistato l'estensione del supporto per una versione precedente di Windows o altri OS?	☐si ☐no

		Se sì, per quali sistemi?
	I sistemi legacy sono isolati da internet e dal resto della rete aziendale?	☐si ☐no Se sì, come?
	Viene effettuato monitoraggio proattivo? Ad esempio Endpoint Detection & Response (EDR)	☒ si ☐no
	L'EDR blocca/isola i sistemi in caso di alert?	☒ si ☐no Se no, quali azioni/procedure di escalation sono prese?
	Si precisa che qualora l'Ente abbia software/hardware end-of-life non isolati da internet e dal resto della rete aziendale, tali strumenti saranno esclusi dalla copertura assicurativa.	

OUTSOURCERS

Quali processi relativi alla gestione delle operazioni e/o della sicurezza dei dispositivi e dei sistemi di rete sono esternalizzati a provider esterni di servizi?

Attività	Fornitore
☒ Server management	DITTA PROXIMA LAB SRL A SOCIO UNICO DI CENE
☒ Network management	DITTA PROXIMA LAB SRL A SOCIO UNICO DI CENE
☒ Security management	DITTA PROXIMA LAB SRL A SOCIO UNICO DI CENE
☐ Data center hosting	
☐ Data processing	
☒ Application management	IL COMUNE UTILIZZA APPLICATIVI SICRAWEB - SICRAWEB EVO DELLA DITTA MAGGIOLI SPA DI SANTARCANGELO DI ROMAGNA (RM) – LA POLIZIA LOCALE UTILIZZA APPLICATIVI SW ANCHE DELLA DITTA OPEN SOFTWARE SRL DI MIRANO (VE)
☒ Alert log monitoring	DITTA PROXIMA LAB SRL A SOCIO UNICO DI CENE
☒ Offsite backup e storage	DITTA PROXIMA LAB SRL A SOCIO UNICO DI CENE
☐ Co- location facility	
☐ Application service provider (ASP)	
☐ Call center/Service desk	
☐ Operational business process	
☐ Sistemi di pagamento	
☐ Altro, specificare:	

SERVIZI IN CLOUD

Sono utilizzati dei servizi in Cloud?
☒ si ☐no

In caso affermativo, indicare:

Partner	Servizi	Nazione in cui sono conservati i dati
CEDEPP SRL DI SALA BAGANZA (PR) OPEN SOFTWARE SRL DI MIRANO (VE) MAGGIOLI SPA DI SANTARCANGELO DI ROMAGNA (RN)	Servizi scolastici (es. mensa, trasporto) Sanzioni codice della strada Applicativi vari SICRAWEB - SICRAWEB EVO	

Sez.2			
SICUREZZA DEI SISTEMI, DELLA RETE E DELLE INFORMAZIONI			
MISURE TECNCHE E ORGANIZZATIVE DI SICUREZZA	**Q.1**	È stata adottata una Politica di Sicurezza delle Informazioni che viene periodicamente aggiornata e resa nota a tutto il personale?	☐si ☒ no
	Q.2	Quali strumenti adotta l'Ente per sensibilizzare i propri dipendenti in materia di sicurezza informatica?	☐ attacchi simulati antiphishing ☒ corsi di formazione ☐ condivisione di articoli, segnalazioni/bollettini via mail ☐ condivisione con i tutti i collaboratori delle specifiche istruzioni per un corretto utilizzo dei sistemi informatici e degli asset aziendali (es. email, internet, social media, supporti rimovibili, regole di comunicazione telefonica, regole di utilizzo laptop in ambienti pubblici, utilizzo di servizi di rete, etc.) ☐ specifiche istruzioni sulle modalità di lavoro in smart working ☐ nessuno
	Q.3	E' presente una procedura che, durante le fasi di conclusione del rapporto lavorativo, preveda un immediato recupero degli elementi di sicurezza (chiavi, tessere etc.), la restituzione degli asset in dotazione e una contestuale disabilitazione delle utenze?	☐si ☒ no (non codificata, ma di fatto esistente)
	Q.4	L'Ente ha implementato un processo di Ict Asset Management, che identifichi tutti gli asset informativi (client, server, apparati di rete, device mobili, applicazioni/dati, etc.) oggetto della copertura assicurativa, nonché l'ownership e le relative responsabilità?	☒ si ☐no
	Q.5	Sono implementate, testate e aggiornate delle configurazioni sicure standard per la protezione dei sistemi operativi e delle applicazioni installate? (es. disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, chiusura di porte di rete aperte e non utilizzate)	☒ si ☐no
	Q.6	L'Ente ha attivato modalità di lavoro agile / smart working?	☒ si, con BYOD: SOLO DURANTE EMERGENZA COVID, NON ATTUALMENTE ☐si, senza BYOD ☐no
	Q.7	In caso di utilizzo di dispositivi personali (BYOD) sono verificati preventivamente i requisiti e le configurazioni di sicurezza?	☒ si ☐no
	Q.8	L'Ente ha reso ai propri collaboratori delle specifiche istruzioni sulle modalità di lavoro in smart working in cui sono dettagliate le basi della sicurezza nel lavoro da remoto?	☐si ☒no
	Q.9	Per le attivazioni su device forniti dall'Ente, sono state implementate le seguenti misure di sicurezza:	☒ disk Encryption ☐DLP ☐ MDM (Mobile device Management) ☒ AV con firewall ☒ Connessione con VPN con 2FA (OTP/authenticator) ovvero altra modalità di connessione attivata (es. accesso a bolla citrix o altra piattaforma di disintermediazione su pagina crittografata (https) ovvero soluzione di virtual desktop)
	Q.10	Per le attivazioni in BYOD, sono state implementate le seguenti misure di sicurezza:	☐ rilascio di agent sulle macchine degli users ☐revoca privilegi amministratore ☒ Verifica presenza AV con firewall con preventiva scansione ☒ Rilascio di soluzione di connessione con VPN con 2FA (OTP/authenticator) ovvero altra modalità di connessione

			attivata (es. accesso a bolla citrix o altra piattaforma di disintermediazione su pagina crittografata (https) ovvero soluzione di virtual desktop)
	Q.11	L'Ente definisce una politica di controllo degli accessi basata sul principio del privilegio minimo?	☒ si ☐no
	Q.12	L'Ente provvede a fornire un identificativo univoco e vieta l'utilizzo di identificativi o utenze condivise (anche a livello di amministratore di sistema)?	☒ si ☐no
	Q.13	L'Ente ha implementato e diffuso una password policy che garantisca e applichi un adeguato livello di complessità e robustezza?	☒ si ☐no
	Q.14	L'accesso ai locali del datacenter è permesso solo al personale autorizzato, dotato di credenziali / badge specifici?	☒si ☐no
	Q.15	[Backup] – Con quale frequenza e modalità è eseguito il back up dei dati?	DAY CON RETENTION 45 gg
	Q.16	[Backup] – Le copie di back up	☒ sono protette in base al livello di confidenzialità delle informazioni che contengono ☐ sono conservate in siti alternativi/secondari
	Q.17	[Backup] - Vengono eseguiti i backup delle configurazioni degli apparati di rete (es. router, firewall ecc.)?	☒ si ☐no
	Q.18	Il sistema di backup prevede delle copie offline?	☒ si ☐no
	Q.19	L'Ente si è dotato di un sistema di correlazione e gestione dei log anche in ottica forense?	☒ si ☐no
	Q.20	In merito alle procedure di Patching Management adottate:	☒ le patch critiche sono aggiornate entro 30 giorni dal loro rilascio ☐le patch non critiche vengono aggiornate entro 6 mesi dal loro rilascio ☐ non esiste una politica definita per la distribuzione delle patch (in questo caso, specificare modalità e tempistiche di aggiornamento adottate) _____
	Q.21	Selezionare quali tra le seguenti misure sono implementate:	☒ antivirus/anti-Malware (inclusa scansione degli allegati di posta e contenuto delle pen drive) ☒ soluzioni di filtraggio della posta elettronica che blocca gli allegati dannosi e file sospetti (antispam) ☒ firewall ☐ application firewall ☒ sistemi di intrusion detection/prevention (IDS/IPS) ☐ SOC (Centro Operativo di sicurezza) ☐SIEM (Security Information And Event Management) ☒ soluzione di filtraggio web che impedisce ai dipendenti di visitare pagine web dannose o sospette note (url/content filtering) ☒ soluzioni di blocco/controllo/rimozione di software installati senza autorizzazione ☒ autenticazione multifattoriale ☒ sistemi crittografici per le comunicazioni da e verso internet (es. adozione di protocolli di tunelling in VPN / SSL o SSH nelle ultime versioni disponibili) ☒ sistemi crittografici per i dispositivi, inclusi quelli rimovibili, in dotazione ai dipendenti ☒ sistemi crittografici per i dati custoditi all'interno delle banche dati informatiche

	Q.22	L'Ente ha approvato e testa regolarmente	☒ Business Continuity Plan ☒ Disaster Recovery Plan ☒ Incident Response Plan ☒ Business Impact Analysis
	Q.23	L'Ente effettua su tutti gli asset rientranti nel perimetro assicurato	☒ Risk Analysis ☒ Vulnerability Assessment ☒ Penetration Test ☐ Altro, specificare
	Q.24	L'Ente ha segregato la rete interna (LAN) in Virtual LAN (VLAN) o domini in base al livello di sicurezza dei processi e informazioni gestite?	☒ si ☐no
	Q.25	Relativamente alle politiche di segmentazione implementate, selezionare ciò che si applica alla postura dell'Ente:	☒ l'Ente ha segmentato la rete in base all'area geografica (e.g.: il traffico tra uffici in luoghi diversi è negato a meno che non sia richiesto per supportare uno specifico requisito aziendale); ☐ l'Ente ha segmentato la rete in base alla funzione aziendale (ad esempio il traffico tra asset che supportano funzioni diverse, ad esempio HR e Finance, è negato a meno che non sia richiesto per supportare uno specifico requisito aziendale); ☐ l'Ente ha implementato regole del firewall host che impediscono l'uso di Remote Desktop Protocol - RDP per accedere alle workstation; ☐ l'Ente ha configurato tutti gli account di servizio per negare gli accessi interattivi; ☐ Nessuno dei precedenti.
	Q.26	L'organizzazione si è dotata di un sistema di selezione dei fornitori che valuti, oltre alla loro solidità finanziaria, anche le loro politiche di cyber security e di trattamento dei dati, e che includa una verifica periodica sul mantenimento dei requisiti richiesti in ingresso?	☐si ☒no
	Q.27	Per i fornitori esiste una procedura di autorizzazione all'accesso diretto o da remoto ai sistemi?	☐si, sono autorizzate connessioni remote via VPN ☒ si, sono autorizzate connessioni remote con autenticazione multifattoriale ☐Nessuna delle precedenti ☐Altro, indicare ☐no

Sez.3

GESTIONE DEI DATI PERSONALI E CONTENUTI MULTIMEDIALI

GESTIONE DELLE ESPOSIZIONI PRIVACY E DELLA MULTIMEDIALITA'

Q.28	Nell'esercizio della propria attività, che tipo di dati personali raccoglie, processa o conserva l'organizzazione?	
	Tipologia dei dati trattati	**Volume dei dati trattati**
	X dati finanziari (carte di credito/debito/ conto corrente)	☐≤100 ☐≤1.000 ☒ ≤100.000 ☐≤1.000.000 ☐≥1.000.000
	X dati personali di terzi Soggetti	☐≤100 ☐≤1.000 ☒ ≤100.000 ☐≤1.000.000 ☐≥1.000.000
	X Informazioni sanitarie	☐≤100 ☒ ≤1.000 ☐≤100.000 ☐≤1.000.000 ☐≥1.000.000
	☐ proprietà intellettuale/copyrights/ segreti commerciali	☐≤100 ☐≤1.000 ☐≤100.000 ☐≤1.000.000 ☐≥1.000.000
Q.29	A chi è attribuita l'attività di gestione della privacy dell'organizzazione?	☐ Società di consulenza o studio legale ☐ Ufficio privacy all'interno dell'Ente (Privacy manager) ☒ Libero professionista
Q.30	L'Ente ha definito e implementato un processo di adeguamento al GDPR?	☒ si ☐no Indicare le principali attività implementate: ☒ aggiornamento informative (dipendenti, clienti, sito internet - inclusa Cookie Policy, ecc.) ☒ formazione dipendenti in materia privacy ☒ processo di raccolta e gestione dei consensi informati ☒ redazione registro dei trattamenti ☒ aggiornamento nomine per il trattamento dei dati (incaricati al trattamento, responsabili, amministratori di sistema, etc.) ☐ trasferimento dati extra UE nel rispetto delle condizioni dalla normativa (art. 44, 45 e 46 GDPR) ☐Altro _____
Q.31	È stato nominato un Responsabile della protezione dei dati (DPO)?	☒ si CLOUDASSISTANCE DI LUIGI MANGILI DI CLUSONE (BG) ☐ no
Q.32	Quali delle seguenti Policy (nelle quali sono anche definiti ruoli e responsabilità) sono state adottate dall'Ente?	☐ Data Breach ☐ Data Retention ☐ DPIA ☐ Gestione delle richieste degli interessati in materia privacy ☒ Regolamento sul corretto utilizzo dei sistemi informatici aziendali ☐ Gestione eventuali reclami sui contenuti creati e pubblicati sui canali online, considerati calunniosi, illegali o in violazione al diritto alla privacy di terzi ☐ Altro, specificare _____

Allegato 1	
VULNERABILITA' NOTA LOG4SHELL	
RILEVAMENTO E GESTIONE VULNERABILITA'	
L'organizzazione esegue o utilizza sistemi vulnerabili a (CVE-2021-44228)?	☐si ☒ no
In caso negativo, è stato confermato dal fornitore di servizi IT?	☒ si ☐no
In caso affermativo, i sistemi sono stati aggiornati o implementate mitigazioni/controlli compensativi a breve termine?	☐si ☐no
A quale % di applicazioni vulnerabili è stata applicata la patch?	
Qual è il piano di mitigazione previsto? (Specificare se è disponibile una cronologia)	
L'organizzazione ha scansionato i sistemi IT vulnerabili alla ricerca di Indicatori di Compromissione (IoC) e successivamente sono state intraprese eventuali contromisure?	☒ si ☐no
Quali misure di rilevamento avete messo in atto?	WithSecure™ Elements Vulnerability Management (RADAR)
Sono state identificate le terze parti critiche che potrebbero essere vulnerabili?	☐si ☒no
Sono stati aggiornati i Firewall per impedire il possibile testo di injection?	☒si ☐no
È stato implementato uno degli strumenti di scansione log4j?	☐si ☒no

Allegato 2

INCIDENTE INFORMATICO

GESTIONE INCIDENTE

In relazione all'incidente occorso indicare:	
Data di accadimento	Nessuna
Breve descrizione dell'incidente	Nessuno
Tempistiche di rilevazione dell'anomalia	☐immediatamente ☐>4ore ☐>12ore ☐>24ore ☐>48 ore ☐ >5giorni Altro, specificare _____
Qual è stato il vettore di ingresso dell'incidente	☐ sito internet ☐ E-mail ☐ Phone ☐ dispositivi aziendali ☐ dispositivi aziendali persi/rubati ☐ dispositivi personali dei dipendenti (BYOD) ☐ abuso Amministratori di Sistema ☐ Rete di terze parti ☐ Altro, specificare
L'incidente ha colpito direttamente l'organizzazione o indirettamente attraverso un incidente informatico subìto da un fornitore di servizi?	☐ direttamente ☐ indirettamente (*Indicare il provider di servizi*)
L'incidente subìto dall'organizzazione ha colpito indirettamente sistemi e infrastrutture di Terzi?	☐ no ☐ si (*Indicare i nominativi dei Terzi coinvolti*)
Quali vulnerabilità sono state rilevate a seguito dell'incidente subìto?	☐ gestione inadeguata delle patch ☐ installazione di software non autorizzato/ versione non aggiornata ☐ sistemi operativi non più aggiornabili (legacy) ☐ gestione inadeguata degli account con privilegi ☐ protezione inadeguata e-mail / browser web ☐ Difese antimalware inadeguate ☐ Configurazioni di sicurezza inadeguate per hardware e software su dispositivi, laptop, workstation, server ☐ Inadeguati sistemi di sicurezza per il controllo degli accessi alla struttura ☐ Controllo inadeguato di porte di rete, protocolli e servizi ☐ Resilienza e / o backup inadeguati di sistemi o file ☐ Dispositivi di rete non protetti (firewall, router, switch) ☐ Manutenzione e monitoraggio dei LOG inadeguati ☐ Penetration & Security Testing inadeguati ☐ Segmentazione di rete inadeguata ☐ Mancanza di consapevolezza/conoscenza del personale ☐ Bug del software

	☐ Difetti hardware ☐ Questioni procedurali ☐ Altro, specificare
Servizi e componenti interessati dall'incidente	☐ Endpoint / client (laptop, PC, sistemi operativi, applicazioni utente, ecc.) ☐ Applicazione / software utente correlato alle banche (vendita, negoziazione, credito, ecc.) ☐ Reti e telecomunicazioni (firewall, router, switch, PBX, ecc.) ☐ Gestione e archiviazione dei dati (file server, database, data warehouse, ecc.) ☐ Applicazioni software aziendali (SAP, Oracle, ecc.) ☐ Piattaforme Internet (server web, server di applicazioni, ecc.) ☐ Altro, specificare
Sistemi interessati dall'incidente	☐ Applicazioni/software ☐ Hardware ☐ Database ☐ Network/Infrastrutture ☐ Altro, specificare
Aree interessate dall'incidente	☐ Direzione ☐ Risorse Umane ☐ Amministrazione e controllo ☐ Contabilità ☐ Altro, specificare
Indicare la durata dell'interruzione dell'attività aziendale conseguente all'incidente occorso	
Indicare l'impatto economico	
Indicare le principali azioni / misure correttive intraprese / pianificate per evitare che l'incidente si ripeta in futuro	
L'Ente, a seguito dell'incidente occorso ha calendarizzato l'esecuzione di un vulnerability assessment o di un penetration test con il supporto di esperti informatici?	☐ si ☐no

DICHIARAZIONI	
	La firma del presente questionario non obbliga il proponente all'acquisto della polizza.
	Il sottoscritto, in forza dei poteri di sottoscrizione e di rappresentanza disgiunta dell'Ente, qui di seguito dichiara che tutte le dichiarazioni e le informazioni rese con il presente questionario sono vere e che non sussistono fatti materiali errati o sottaciuti. Per fatto materiale si intende un qualsiasi accadimento che potrebbe influenzare l'accettazione o la valutazione del rischio.
	Il sottoscritto accetta che il presente questionario, qualsiasi allegato allo stesso o informazione fornita con lo stesso, e tutte le altre informazioni rese e/o richieste, potrebbero costituire la base di un eventuale e futuro contratto di assicurazione. Il sottoscritto conseguentemente si obbliga ad informare l'Assicuratore di qualsiasi modifica materiale di qualsiasi informazione, dichiarazione, rappresentazione o fatto presentati in questo questionario, che si verifichino prima o dopo la data di decorrenza della copertura assicurativa.

Luogo e Data

_____

Titolo/Funzione dell'incaricato e Firma

_____