CYBER INSURANCE PROPOSAL FOR

Ridgedale Local School District

PRESENTED BY HYLANT

LAURIE MANNING

HYLANT

811 Madison Ave, Toledo, OH 43604
P *419-255-1020* ***F*** 419-255-7557

hylant.com

TABLE OF CONTENTS

ACCOUNT & EXPOSURE SUMMARY

School District: Ridgedale Local School District
Address: 3103 Hillman Ford Rd Morral, OH 43337

Estimated Annual Revenue (next 12 months): $8,800,000
Full Prior Acts: Yes
NAICS Code/Description: Primary and Secondary Schools (Education)

PRICING SUMMARY

	CFC Alternate Expiring	CFC Alternate Option #1	OSP Renewal Option #2
Total Payable	**$3,255.00**	**$3,480.00**	**$1,605**
Premium Carrier Fee SL Fees & Taxes	$3,255.00 N/A N/A	$3,480.00 N/A N/A	$1,605 N/A Exempt
Coverage Type	Admitted	Admitted	Non-Admitted
Limit – Occurrence / Agg	$1M / $1M	$1M / $1M	$1M / $5M
Retention	$10,000	$5,000	$25,000
Wait Period	8 Hours	8 Hours	12 Hours
Subjectivities		1. Request to Bind Coverage 2. Confirm that you have downloaded and registered for CFC's Response Mobile App	1. Request to Bind Coverage 2. Confirm that you have read and understand Coverage Notes on page 3.
Additional Limit Options		$2M xs $5K for $4,655.00	N/A

Price and coverage may change based on application answers provided.
Please carefully review carrier quote information as this comparison is a simplified view and may not include all the information required to make a purchase decision. Please note that quotes expire after 60 days or 7/1/2023, whichever comes first.

COVERAGE OPTIONS

	CFC Alternate Expiring	CFC Alternate Option #1	OSP Renewal Option #2
3rd Party Coverage			
Network Security Liability	$1M	$1M	$1M
Privacy Liability	$1M	$1M	$1M
Regulatory Liability	$1M	$1M	$1M
PCI-DSS Liability	$1M	$1M	$1M
Media Liability	$1M	$1M	$1M
1ST Party Coverage			
Business Interruption (BI)	$1M	$1M	$1M
BI System Failure	$1M	$1M	$1M
Dependent BI	$1M	$1M	$1M
Dependent BI System Failure	$1M	$1M	$1M
Data Restoration / Recovery	$1M	$1M	$1M
Extortion / Ransomware	$1M	$1M	$1M
Bricking	$1M	$1M	$1M
Reputational Harm	$1M	$1M	-
Telephone Hacking	$250K	$250K	$1M
Social Engineering	$250K	$250K	$50K
Customer Payment Fraud	$50K	$50K	-
Breach Costs Outside the Limit	$1M	$1M	-
Policy Aggregate	**$1M**	**$1M**	**$5M**
Coverage Notes	This is an Independent Policy purchased solely by the school district and for use solely by the school district and insureds named on the policy.		A **$250K Ransomware Event Sublimit** will be allocated to schools without the below controls ***at the time of claim:*** 1. MFA for Remote Access 2. MFA for Email Access 3. MFA for Administrative, Privileged Access 4. EDR on 95%+ of Endpoints This is a Shared/Group policy purchased by the Ohio School Plan and its participating members. This policy is for the use of the school districts who participate in the policy and as specifically listed as named insureds on the policy. Claims are subject to a $1M limit per claim. The policy is subject to a maximum aggregate of $5M. Once the policy aggregate is met, no coverage will remain, even if participants have not had a claim.

COVERAGE DEFINITIONS

Coverage Type and Carrier rating

Admitted carriers are insurers that have been granted a license by a state's department of insurance to do business within that state. Admitted Carriers contribute to their state's guaranty fund which provides relief for insureds, based on state specific limits, in the case of an insurers' insolvency.

Surplus lines insurers are referred to as non-admitted carriers because they are not licensed in the state of the insured's principal place of business or residence. While the surplus lines market is regulated differently than the admitted market, in order to provide the flexibility necessary to cover the hard-to-place risks, it is a regulated marketplace. State surplus lines insurers' capitalization requirements are generally higher than admitted carriers which allows for greater protection for policyholders.

AM Best uses a letter grade scale ranging from A++ to D in order to rate an insurers financial strength. A rating of "A" or higher means that the insurer has "excellent ability to meet their ongoing insurance obligations."

Issuing insurer

The insurance company providing the coverage and paying claims.

Limit

The total amount of losses that can be paid under an insurance policy.

Retention

An insured's assumption of risk of loss through noninsurance, self-insurance, or deductibles.

Deductible

The amount an insurer will deduct from the loss before paying up to its policy limits.

Air-Gapped

Air gap means offline and not connected to your network or the Internet. An air-gapped backup is a copy of your data that is kept offline so that it cannot be accessed by a hacker. This protects it from almost any type of cybersecurity threat. They are also called an offline strategy. This is designed to protect you from almost any type of ransomware.

EDR

Endpoint Detection and Response, EDR for short, is a security solution that uses a combination of continuous monitoring and data collection on end user devices to detect potential cyber threats

MFA

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.

Cyber Risk Assessment

A third-party scan of your attack surface (endpoints) for vulnerabilities and/or suggested security improvements. These scans mimic how threat actors would view your network and are meant as a proactive aid to bolster security posture.

24/7 Security Monitoring

The carrier's proactive scanning of your network, throughout the policy period, in effort to thwart new risks and alert you of potential vulnerabilities.

Preferred Partner Enhanced Coverage

An endorsement added to your policy which includes bespoke coverage enhancements negotiated for policyholder benefit.

3RD PARTY COVERAGE

Network Security and Privacy Liability

Protects the policyholder against losses for the failure to protect a customer's personally identifiable information (such as social security number, credit card numbers, medical information and passwords) from various cyber-attacks.

3rd Party Coverage

Helps pay for lawsuits caused by data breaches on a client’s network or systems.

Media Liability

Coverage for defamation, invasion of privacy, infringement of copyright and plagiarism resulting from a cybersecurity event.

1ST PARTY COVERAGE

Extortion / Ransomware

A type of cyber-attack that blocks access to a victim's data, website, client services systems or other critical resources. The ransomware is then used to demand payment of monies in return for unblocking access to the victim's resources.

Bricking

Insure against the loss of use or functionality of hardware (such as servers) as a result of a hacking event.

1st Party Coverage

In accordance with the terms of the policy, coverage for data breaches and losses to your own network or systems

Reputational Harm

Typically covers the costs of public relations, media purchasing and other related costs to mitigate harm to a brand’s reputation due to a cybersecurity event.

Crypto Jacking

Cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets or servers) to mine for cryptocurrency.

Social Engineering

A cybercrime technique that manipulates people in an online environment to divulge sensitive, personal information in good faith – such as account numbers, passwords, or banking information

Contingent / Dependent Business Interruption

Financial loss resulting from outage of a 3rd party’s system which causes disruption to your system. These entities can include vendors, suppliers, and other similar entities. Refer to policy details for specifics

Contingent / Dependent System Failure

Financial loss resulting from outage of a 3rd party’s system which causes disruption to your system. These entities can include vendors, suppliers, and other similar entities. Refer to policy details for specifics.

Invoice Manipulation

A form of cybercrime where a fraudulent invoice is manipulated or created and causes remittance of payment to a fraudulent account

CLAIMS SCENARIOS

Ransomware

A company that manufactures metal product components was the victim of a cyber-attack that stole control of their industrial control systems. This completely halted their production line, creating a massive business interruption and delaying distribution schedules for their partners. The hackers took control of the robotic equipment in the factory and forced the hardware to inflict damage to the equipment and destroy the components in the midst of production. The extensive business interruptions and physical property damage would have been an incredibly costly situation for the manufacturer, had they not had a cyber insurance policy. Their cyber policy covered the business interruption expenses, financial demands made by their production partners whose processes were also delayed, and costs to repair the damaged factory, totaling almost $1M in losses.

Social Engineering

A bad actor impersonated the head of accounting for a manufacturing company and sent an email to two existing vendors to change the wiring information they had on file to receive payments. When the vendors did not receive their payments, they alerted the manufacturer. After being alerted about the fraudulent email, the manufacturer was able to enlist their cyber security insurance to remedy the situation. The carrier covered the costs of wire transfers and provided social engineering training for all employees with a company email, for a total of $250,000.

Privacy Related

A clothing manufacturer was the victim of a data breach when a hacker bypassed the security system on their online ordering platform. The manufacturer only discovered this when they were notified by the federal government that a hacker had been arrested and had accounts linked back to the manufacturer that showed he was in possession of credit card information for 5,000 of the company's customers. The company enlisted the help of their cyber insurance carrier to hire a forensics team, which determined the hacker had been in their system for four months, steadily stealing customer names, addresses, credit card numbers and account passwords. Extensive measures were needed to remedy the situation, including notifying all affected customers, paying for a free year of credit monitoring, as well as hiring a public relations team to repair their damaged public reputation. Without cyber insurance, the company could have expected to pay $300,000 in legal fees, $200,000 in investigation and forensics costs, $150,000 in fines and penalties, and $40,000 in customer notification, reimbursement and crisis management.