NYMIR Cyber Liability Insurance New Business Application

NOTICE: THIS POLICY'S LIABILITY INSURING AGREEMENTS PROVIDE COVERAGE ON A CLAIMS-MADE AND REPORTED BASIS AND APPLY ONLY TO CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR EXTENDED REPORTING PERIOD, IF PURCHASED, AND REPORTED TO THE INSURER IN ACCORDANCE WITH THE TERMS OF THE POLICY. THE LIMIT OF LIABILITY AVAILABLE TO PAY JUDGMENT OR SETTLEMENTS WILL BE REDUCED AND MAY BE EXHAUSTED BY THE AMOUNTS INCURRED FOR LEGAL DEFENSE AND CLAIMS EXPENSES. FURTHERMORE, AMOUNTS INCURRED FOR LEGAL DEFENSE AND CLAIMS EXPENSES WILL BE APPLIED AGAINST THE RETENTION.

IF A POLICY IS ISSUED, THIS APPLICATION WILL ATTACH TO AND BECOME PART OF THE POLICY. THEREFORE, IT IS IMPORTANT THAT ALL QUESTIONS ARE ANSWERED TRUTHFULLY AND ACCURATELY. READ AND REVIEW THE ENTIRE APPLICATION CAREFULLY BEFORE SIGNING.

Cyber Quote(s) Requested: ☐$250k ☐$500k ☐$1M ☐$2M

Municipality Name:

Municipal Website Address:

Municipal Contact Name: Title:

Email Address: Telephone Number:

Name of IT Provider/ IT Contact (If Applicable):

Email/ Phone Number of IT Provider/ IT Contact (If Applicable):

Approximate Number of Employees: Full-time Part-time

Complete each question for the remainder of the application with the Insured/Municipality in mind.

Data Security & Governance

1. Please approximate the following for the Municipality:

   Number of Active Email Addresses:

   Number of Desktop Computers:

   Number of Laptops:

2. Does the Municipality use third-party vendors for IT services or software solutions: ☐Yes ☐No
   If YES, list vendors and services:

3. Do you evaluate third-party vendors that access sensitive data (e.g., harmless and indemnification agreements, risk assessments, or security documentation)? ☐Yes ☐No ☐N/A (No external vendors used)
4. Do you backup all mission critical systems and data? ☐ Yes ☐ No
   If YES, please provide the following information:
   a. How frequently do you back up? ☐Daily/nightly ☐Weekly ☐Less frequently than weekly
   b. Which of the following back-up solutions do you employ? (select all that apply)
      ☐Local ☐Network drives ☐Tapes/ disks ☐Offsite ☐Cloud
   c. Which controls are in place to protect backups (select all that apply):

      ☐Encryption
      ☐Disconnected from the Network (Air Gapped)
      ☐Virus Malware Scanning
      ☐Credentials are Stored Separately
      ☐Multi-Factor Authentication (MFA)
      ☐Immutable

   d. How often are backups tested, restored, or verified ☐Annually ☐Quarterly ☐Other ☐Never
5. Indicate which of the following for which Multi-Factor Authentication (MFA) has been implemented (select all that apply):
   Remote Network Access (e.g., VPN) ☐ Yes ☐ No ☐ N/A (No remote access allowed)

Web-based Email Access ☐ Yes ☐ No

Accessing Personal Devices ☐ Yes ☐ No ☐ N/A (No personal devices allowed to access municipal data or email)

Administrative or Privileged User Accounts Required ☐ Yes ☐ No

Online Banking/ Financial Transactions ☐ Yes ☐ No ☐ N/A (Not offered by bank)

6. Do you have email security controls in place? ☐ Yes ☐ No

If YES, which controls are in place (select all that apply):

Email filtering tool to detect and/or block SPAM, malicious links, and attachments is use ☐ Yes ☐ No

A secure email gateway in place (e.g., Microsoft Defender for O365, Proofpoint, Barracuda, Cisco)☐ Yes ☐ No

Email authentication methods (e.g., SPF, DKIM, DMARC) implemented ☐ Yes ☐ No

Sandboxing or analysis for malicious attachments ☐ Yes ☐ No

MFA ☐ Yes ☐ No

Please specify the web-based email platform in use (e.g., Office 365/Outlook, Google) and/ or any secondary email security software (e.g., Barracuda, Proofpoint):

7. Does the Municipality allow remote access to the municipal network? ☐ Yes ☐ No

If YES, how is remote network access secured (select all that apply):

☐Use of a Virtual Private Network (VPN) with Multi-Factor Authentication (MFA).

☐Restriction or security measures in place for:

☐Remote Desktop Protocol (RDP - Port 3389)

☐Server Message Block (SMB - Ports 139 & 445)

☐Secure Shell (SSH - Port 22)

☐Other

8. Are endpoint (PC's, Laptops, Smartphones, Tablets, etc.) security controls in place? ☐Yes ☐No

If YES, which controls are in place for endpoint security (select all that apply):

☐Password/passcode protected

☐Encryption

☐Traditional or next generation firewalls enabled/turned on

☐Traditional or next generation antivirus products on all endpoints

☐Endpoint Detection and Response (EDR) 24/7/365 on all endpoints

☐Intrusion Detection System (IDS) or Managed Detection and Response (MDR)

Please specify the provider used (e.g., *Sophos, Huntress, CrowdStrike, Malwarebytes, Bitdefender, Norton, and Windows Defender):*

9. Are passwords required to access workstations, systems, and software? ☐ Yes ☐ No

If YES, please describe your current password requirements or policy (e.g., minimum length, character types, expiration policy):

10. Are access control policies enforced? ☐ Yes ☐ No

If YES, which controls are in place for endpoint security *(select all that apply):*

☐ Role-based access / principle of least privilege

☐ Zero trust architecture

☐ Removal of admin rights for non-IT users

☐ Timely deactivation of access for terminated employees or expired accounts

☐ Regular auditing and monitoring of user access

☐Other

11. Does the Municipality update and push patches in a timely manner? ☐ Yes ☐ No
12. Are there any end-of-life or end-of-support systems/ software in use? ☐ Yes ☐ No

If YES,

Is it segregated from the network? ☐ Yes ☐ No

What end-of-life or legacy system(s) are used? Why? Will they be retired?

13. Indicate which of the following controls have been implemented and consistently enforce with respect to Electronic Funds Transfer (EFT) (select all that apply):
    - ☐No EFTs are conducted
    - ☐Secondary verification via callback procedure or unique verification code to verify funds transfer requested or changes to banking information
    - ☐Dual sign-off prior to funds transfers exceeding a specified dollar value (e.g., $10,000)
14. Does the Municipality secure public Wi-Fi? ☐Yes ☐No ☐N/A (No Public Wi-Fi)

If YES, which controls are in place (select all that apply):

- ☐User authentication required before access
- ☐Public Wi-Fi is segmented from the internal municipal network
- ☐Strong encryption protocols are used (e.g., WPA2, WPA3)
- ☐Firewall is configured to monitor and filter traffic
- ☐Other ____

15. Is employee security awareness training, including phishing training, provided for those that use technology as part of their duties?
    ☐ Annually ☐Semi-Annually ☐Monthly ☐Other ____ ☐Never
16. Which security framework do you align with? (select all that apply)
    ☐NIST ☐ISO ☐27001 ☐SOC ☐CIS ☐Other ____

Claims History and Loss Information

1. Has the Municipality experienced any of the following situations in the last three years? ☐ Yes ☐ No

   Privacy Incident and/or claims? ☐ Yes ☐ No

   Network Incident and/or claims? ☐ Yes ☐ No

   System Failure Incident and/or claims? ☐ Yes ☐ No

   Cyber Crime Incident and/or claims? ☐ Yes ☐ No

   Media Incident and/or claims? ☐ Yes ☐ No

   ***If YES to any of the above**, please provide a complete description of the incident in an addendum to this application, including costs, losses or damages incurred or paid, and any corrective measures to respond to such incident.*

2. Are you aware of any fact, circumstance, or situation involving the Municipality that you have a reason to believe will cause a **Privacy Incident, Network Security Incident, System Failure Incident, Cyber Crime Incident, Media Incident or Claim**? ☐ Yes ☐ No

   ***If YES to any of the above,** please provide a complete description of the facts, circumstances, situations, events or transactions in an addendum to this application.*

The Municipality understands and agrees that if any fact, circumstance, situation, event or transaction exists, whether or not disclosed, the proposed insurance will not afford coverage for any claim or loss arising from such fact, circumstance, situation, event or transaction.

Representations, Fraud Warnings, and Signatures

THE SIGNING OF THIS APPLICATION DOES NOT BIND THE INSURER TO OFFER, NOR THE APPLICANT TO PURCHASE, THE INSURANCE. IT IS AGREED THAT THIS APPLICATION, INCLUDING ANY MATERIAL SUBMITTED THEREWITH, SHALL BE THE BASIS OF INSURANCE AND BE CONSIDERED PHYSICALLY ATTACHED TO AND PART OF THE POLICY, IF ISSUED. THE INSURER WILL HAVE RELIED UPON THIS APPLICATION, INCLUDING ANY MATERIAL SUBMITTED THEREWITH, IN ISSUING THE POLICY.

THE UNDERSIGNED AUTHORIZED REPRESENTATIVE OF THE APPLICANT DECLARES THAT TO THE BEST OF HIS/HER KNOWLEDGE AND BELIEF, AFTER REASONABLE INQUIRY, THE STATEMENTS SET FORTH IN THE ATTACHED APPLICATION FOR INSURANCE AND IN ANY MATERIALS SUBMITTED WITH THIS APPLICATION ARE TRUE AND COMPLETE AND MAY BE RELIED UPON BY THE INSURER. IF THE INFORMATION IN THE APPLICATION CHANGES PRIOR TO THE INCEPTION DATE OF THE POLICY, THE APPLICANT WILL NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY MODIFY OR WITHDRAW ANY OUTSTANDING QUOTATION. THE INSURER IS AUTHORIZED TO MAKE INQUIRY IN CONNECTION WITH THIS APPLICATION.

THE INFORMATION REQUESTED IN THIS APPLICATION IS FOR UNDERWRITING PURPOSES ONLY AND DOES NOT CONSTITUTE NOTICE TO THE INSURER UNDER ANY POLICY OF ANY ACTUAL OR POTENTIAL CLAIM OR LOSS.

Applicant Signature