NYMIR Cyber Liability Insurance Renewal 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.

Municipality Name: _____

Municipal Website Address: _____

Municipal Contact Name: _____ Title: _____

Email Address: _____ Telephone Number: _____

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

1. Have there been any changes to your municipality's cybersecurity practices, controls, systems, or risk exposure since completing last year's NYMIR Cyber Insurance Application? ☐ Yes ☐ No

   *If **Yes**, please describe the changes in detail in an addendum and attach any supporting documentation (e.g., updated policies, vendor contracts, incident response plans).*

2. Indicate which of the following controls the Municipality has implemented **(check all that apply)**:

Backups

Backups performed ☐Daily/nightly ☐Weekly ☐Less frequently than weekly ☐Never

Backups disconnected from the network or air gapped ☐ Yes ☐ No

Backups tested, restored, or verified ☐Annually ☐Semi-Annually ☐Quarterly ☐Other _____ ☐Never

Backups in the cloud are protected with Multi-Factor Authentication (MFA) ☐ Yes ☐ No ☐ N/A (No cloud backups)

Multi-factor Authentication (MFA)

MFA for remote network access (e.g., VPN) ☐ Yes ☐ No ☐ N/A (No remote access allowed)

MFA for web-based email access ☐ Yes ☐ No

MFA for personal devices ☐ Yes ☐ No ☐ N/A (No personal devices allowed to access municipal data or email)

MFA for administrative or privileged user accounts ☐ Yes ☐ No

MFA for online municipal banking or financial transactions ☐ Yes ☐ No

Email Security

Spam filtering tools in 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

Inbound email attachments analyzed for malicious behavior using sandboxing or similar tools. ☐ Yes ☐ No

Electronic Funds Transfers (EFTs)

All EFTs, changes to banking information, and vendor updates verified through a secondary means (e.g., phone call confirmation) ☐ Yes ☐ No ☐ N/A (No EFTs)

Training

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

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 renewal 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