GSMJIF 2017 CYBER LIABILITY QUESTIONNAIRE

Full Name of Applicant: _____

I. MANAGEMENT OF CREDIT CARD EXPOSURES

1. Does the Applicant accept credit cards for goods sold or services rendered?

   A. Is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)?

   If the Applicant is not compliant with applicable data security standards, please describe the current status of any complaince work and the estimated date of completion: _____

   _____

II. COMPUTER SYSTEMS CONTROLS

1. Does the Applicant conduct training for every employee user of the information systems in security issue and procedures for its computer systems?

2. Does the Applicant have a written information security policy in place?

3. Does the Applicant have a program in place to test or audit security controls on an annual or more frequent basis?

   If yes, please summarize the scope of such audits and/or tests: _____

   _____

4. Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company?

5. Does the Applicant have and enforce polcies concerning when internal and external communication should be encrypted?

   A. Are all laptop computers and portable media (e.g. “thumb drives” backup tapes) protected by encryption?

6. Does the Applicant have and enforce polcies including installation of software “patches”?

   If Yes, are critical patches installed within 30 days of release?

7. How often are anti-virus software signatures updated? Automatic Updates Weekly Monthly Other

8. Does the Applicant have and regulary maintain and/or update a Firewall?

9. Has the Applicant suffered and known intrusions (i.e., unauthorized access or security breach) or denial of service attacks relating to its computer systems in the most recent three year tome period from the date of this application?

   If yes, describe any such intrusions or attacks, including any damage caused by any such intrusions, including lost time, lost business income, or costs to repair any damage to systems or to reconstruct data or software, describe the damage that occurred, and state value of any lost time, income and costs of any repair or reconstruction: _____

   _____

10. Does the Applicant provide training to key employees regarding the Privacy Policy and the handling of personally idetifiable information

GSMJIF
Garden State Municipal Joint Insurance Fund

GSMJIF 2017 CYBER LIABILITY QUESTIONNAIRE

III. TYPES OF PRIVATE INFORMATION ACCESSED, PROCESSED OR STORED			
Does the Applicant typically access, process and or store:			
1. Names and addresses?	Employees	Residents	Employees and residents
2. Financial account information?	Employees	Residents	Employees and residents
3. Drivers license numbers?	Employees	Residents	Employees and residents
4. Social security numbers?	Employees	Residents	Employees and residents
5. Protected health information?	Employees	Residents	Employees and residents
6. Please provide a rough percentage of the information stored in each format.	Electronically stored _____% Paper Format _____% **Must total to 100%*		
7. Do all employees have access, or is access limited to certain individuals?	Describe: _____ _____		

IV. MISCELLANEOUS
1. Are Third-Party Service Providers used for processing payments on the Applicant's behalf?
2. Does the Applicant currently sponsor publi access Wi-Fi for residents (e.g., "hotspots")?

V. WEBSITE MEDIA CONTENT
1. Do you have a procedure for review and approval of material published to pages on your Internet site as well as social media messages posted on behalf of the municipality in order to avoid the publication of infringing or improper material?

Completed By:	_____
Signature:	_____
Title:	_____
Date Completed:	_____