Mid Atlantic Cyber Application

NOVATAE RISK GROUP

***Please note**other apps may be needed based on the business operations*

Name: _____

Mailing Address: _____

Location Address: _____

Contact Name: _____

Phone number: _____ Email Address: _____

Year Business Established: _____ FEIN: _____

# of Employees: _____

Description of Operations: _____

_____

Website: _____

Cyber limit requested: _____ Retention: _____

Domestic Revenue: _____ Foreign Revenue: _____

Projected Next Fiscal year Global Revenues: _____

Number of protected records: (please select one)

- ☐ Under 10,000
- ☐ Under 100,000
- ☐ Under 250,000
- ☐ Under 500,000
- ☐ Under 1,000,000
- ☐ Over 1,000,000

Does the applicant currently or will the applicant potentially operate as any of the following:

- ☐ Accreditation services provider
- ☐ Adult content provider
- ☐ Credit bureau
- ☐ Cryptocurrency exchange
- ☐ Cybersecurity products and services
- ☐ Data aggregator/broker/warehouse
- ☐ Direct marketer
- ☐ Gambling services provider
- ☐ IT managed services provider
- ☐ Mfg of life safety products/software
- ☐ Media production company
- ☐ Payment processor
- ☐ Social media
- ☐ Surveillance (physical or digital)
- ☐ Third party claims administrator
- ☐ None of the above

Does the applicant derive more than 50% of its revenue from technology products and services (software, electronics, telecom)?

☐ Yes ☐ No

Does the applicant accept payment card (credit or debit card) transactions?

☐ Yes ☐ No

If yes, Is the applicant PCI compliant?

☐ Yes ☐ No

Does the applicant deal with protected health information as defined by HIPPA

☐ Yes ☐ No

If yes, is the applicant compliant with HIPAA and HITECH Act?

☐ Yes ☐ No

Which of the following IT Security controls does the applicant have in place? *(check all that apply)*

☐ Antivirus and firewalls

☐ Encryption of sensitive data at rest and in transit

☐ Encryption and endpoint protection mobile computer devices

☐ Formal vulnerability management and software patching producers

☐ Formal data backup and recovery procedures in place and tested periodically

☐ Formal cyber incident response plan in place tested periodically

☐ Multifactor authentication on corporate email

☐ Multifactor authentication on corporate network, systems, and VPNs

Does the applicant rely on cloud computing, software-as-a-service, or any other outsourced computer hosting for revenue-generating operations?

☐ Yes ☐ No

Are there any scheduled providers to add for contingent business income?

☐ Yes ☐ No

Does the applicant intend to purchase E&O and/or media coverage on a separate and distinct policy?

☐ Yes ☐ No

Does the applicant provide consumer products or services?

☐ Yes ☐ No

Has the applicant obtained legal review of it's use of trademarks, including domain names?

☐ Yes ☐ No

Has your business suffered a cyber-related loss in the past 12 months?

☐ Yes ☐ No

Do you have data retention and disposal policies?

☐ Yes ☐ No

Do you monitor your network in real time for possible intrusions or abnormalities?

☐ Yes ☐ No

Do you or a third-party provide security awareness and phishing training to employees at least annually?

☐ Yes ☐ No

If you process fund transfer requests, do you confirm the instructions via a method other than the original means of the instruction (for example calling an individual to confirm the wire transfer after they sent an email)?

☐ Yes ☐ No

Do you routinely review all material (including digital content) for intellectual property and privacy compliance prior to any publication, broadcast, distribution or use?

☐ Yes ☐ No

Do you require indemnification or hold harmless agreements from third parties (outside advertising agency) when contracting with them to create or manage content on your behalf?

☐ Yes ☐ No

Do you have place in place to limit disruption to your business operations in the event of a cyber incident?

☐ Yes ☐ No

Have you tested the successful restoration and recovery business-critical applications and data from backups in the last 6 months?

☐ Yes ☐ No

Do you have processes established around identity and access management, including privileged access management, in order to limit the number of users with access to critical corporate data?

☐ Yes ☐ No

Do you perform assessments or audits at least annually to ensure that third-party vendors meet necessary security requirements?

☐ Yes ☐ No

Do you have dedicated internal personnel that actively monitor security operations 24/7, and/or do you alternately use a third-party vendor for such purposes?

☐ Yes ☐ No

Do you have processes in place that regularly review commercial or proprietary software for known security vulnerabilities, and subsequently patch or upgrade such software?

☐ Yes ☐ No

If needed, can highly critical security vulnerabilities be patched within 72 hours by either you or a third-party?

☐ Yes ☐ No

Do you maintain and regularly update digital asset inventory (including hardware such as computers, network devices, and printers, software, and data?

☐ Yes ☐ No