Measured

Trust, quantified.

CyberGuard 2023

Cyber Insurance Application

Measured
Trust, quantified.

Primary Location

Company	Enter Here
Name Address	Enter Here
City	Enter Here
State	Enter Here
ZIP Code	Enter Here

Organization Profile

Description of Business Activities	Enter Here
Industry NAICS code	Enter Here
Year Founded	Enter Here
Employee Count	Enter Here
All owned or operated Website(s) of applicant:	Enter Here
Annual Revenue *(Previous financial year)*	$ Enter Here
Annual Revenue *(Current financial year)*	$ Enter Here
Annual Revenue *(Next financial year projected)*	$ Enter Here

Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed?

Yes ○
No ○

If 'Yes', please explain: Enter Here

Attestations

EMAIL SECURITY, INFRASTRUCTURE SECURITY, BACKUP & RECOVERY POLICIES, sections must be completed by the individual ('you') or teams responsible for the Organizations network security, protocol, and regulatory compliance.

Position, Name, email address, phone number, and list an alternative contact in your absence.

Primary Name	Enter Here	Alternate Name	Enter Here
Primary Title	Enter Here	Alternate Title	Enter Here
Primary Email	Enter Here	Alternate Email	Enter Here
Primary Phone	Enter Here	Alternate Phone	Enter Here

FINANCIAL FRAUD, MEDIA sections must be completed by the Organizations CFO (or similar) and Legal Counsel (or similar) – if neither positions exist within the Organization, please list the similar position:

Contact Name	Enter Here
Title	Enter Here
Contact Email	Enter Here

Data

Confirmation of the number of unique PII/PHI/PCI records which are stored and or processed by the Applicant:

Number of PII records	Enter Here
Number of PHI records	Enter Here
Number of PCI records	Enter Here

Private or sensitive information includes any information or data that can be used to uniquely identify a person, including, but not limited to, social security numbers or other government identification numbers, payment card information, drivers' license numbers, financial account numbers, personal identification numbers (PINs), usernames, passwords, healthcare records and email addresses.

Confirmation that all data reference in Question 1 is encrypted:

a. While at rest in the Applicant's databases or on the Applicant's network — Yes ○ No ○

b. While in transit in electronic form — Yes ○ No ○

c. On electronic portable devices — Yes ○ No ○

d. On employee-owned devices — Yes ○ No ○

e. In the care, custody, and control of a third party service provider — Yes ○ No ○

Is the Applicant subject to the General Data Protection Regulation (GDPR)? — Yes ○ No ○

If Yes, is the Applicant currently compliant with GDPR? — Yes ○ No ○

Does the Applicant collect, store, host, process, control, use or share any biometric information or data, such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? — Yes ○ No ○

Confirmation of PCI – DSS Compliance. If no credit cards are processed by your organization, select N/A. — Yes ○ No ○ N/A ○

Measured
Trust, quantified.

Email Security

Please list the Applicant's third-party Secure Email Gateway Vendor:

Insert vendor name Enter Here

If the Applicant utilizes Office 365 within the organization for email, confirm that Microsoft Defender for Office 365 has been configured as a Secure Email Gateway: Yes ○ No ○

Is the Applicant's email configured to use the following:

a. SPF ○ Yes ○ No

b. DKIM ○ Yes ○ No

c. DMARC ○ Yes ○ No

For all employees with email access, confirm that Multi-factor Authentication (MFA) is always utilized via a web-application or non-corporate device. Yes ○ No ○

Infrastructure Security

Has the Applicant configured multi-factor authentication (MFA):

a. For users who have access to highly confidential information and/or administrative rights to company hardware and/or software? Yes ○ No ○

If Yes/No does not apply, or if you wish to provide more information, please provide clarity using the below text box:

Enter Here

b. For remote access to your network? Yes ○ No ○

If Yes/No does not apply, or if you wish to provide more information, please provide clarity using the below text box:

Enter Here

c. Administrator access to cloud providers including Software-as-a-Service (SaaS) Yes ○ No ○

If Yes/No does not apply, or if you wish to provide more information, please provide clarity using the below text box:

Enter Here

Measured
Trust, quantified.

Infrastructure Security

Has the Applicant implemented a hardened baseline configuration across servers, laptops,desktops and managed mobile devices?
- Yes ○
- No ○

Does the Applicant have a business continuity and/or disaster recovery plan specifically addressing IT incidents?
- Yes ○
- No ○

Does the Applicant have Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) in the business continuity or disaster recovery plan?
- Yes ○
- No ○

Does the Applicant have centralized log collection and management that allows for review of all access and activity on the network?
- Yes ○
- No ○

Has the Applicant deployed an endpoint protection (EPP) solution across the network covering 100% of endpoints?
- Yes ○
- No ○

Please list your EPP provider:

Enter Here

Has the Applicant deployed an endpoint detection and response (EDR) solutions across the network covering 100% of endpoints?
- Yes ○
- No ○

Please list your EDR provider:

Enter Here

If Yes/No does not apply, or if you wish to provide more information, please provide clarity using the below text box:

Enter Here

Does the Applicant segregate "end-of-life" or "out-of-support" hardware and/or systems? from the network?
- Yes ○
- No ○

"N/A" if the applicant does not host any "end-of-life" or "out-of-support" hardware and/or systems.
- N/A ○

Has the Applicant established a Security Operations Center (SOC)?
- Yes ○
- No ○

What is the Applicant's target time to deploy 'critical' patches?
- Within 1 day ○
- Within 7 days ○
- Within 30 days ○

Backup & Recovery Policies

Critical data is those on which the success of business processes and corresponding business applications rely. This includes any data for which you are legally responsible and any data which is relied upon for the uptime or functionality of your organization.

Confirmation that the Applicant's critical data backups are:

a. Segmented from and inaccessible through the organizations network

- Yes ○
- No ○

b. Able to be restored and that this restoration process has been tested within the past 6 months

- Yes ○
- **No** ○

c. Encrypted

- Yes ○
- No ○

If Yes/No does not apply, or if you wish to provide more information, please provide clarity using the below text box:

Enter Here

How frequently does the Applicant back up critical data and/or key configurations?

- Continuously ○
- Daily ○
- Weekly ○
- Monthly ○

If Yes/No does not apply, or if you wish to provide more information, please provide clarity using the below text box:

Enter Here

In the last 6 months, has the Applicant tested the integrity of back-ups for malware and successful restoration of critical data and/or key configurations?

- Yes ○
- No ○

Measured
Trust, quantified.

Financial Fraud

Before transferring any funds or accepting any changes to payment instructions, does the Applicant's finance department or similar always confirm the instructions via a method other than the original means of the instruction.

Yes ○
No ○

Do the Applicant's procedures require review of all requests by a supervisor or next-level approver before processing fund transfer instructions?

Yes ○
No ○

Does the Applicant verify all requests to change customer, vendor, or supplier details via a direct phone call?

Yes ○
No ○

Does the Applicant conduct IT Security training (including phishing/social engineering email training) on an annual basis for all employees?

Yes ○
No ○

Please list your IT Security training provider: Enter Here

If Yes/No does not apply, or if you wish to provide more information, please provide clarity using the below text box:

Enter Here

Media

Does the Applicant have a process in place that includes legal review of content prior to publishing on its websites, social media accounts, or other promotional materials?

Yes ○
No ○

Does the Applicant employ a process for responding to libelous, IP infringement and third-party violation rights complaints?

Yes ○
No ○

Loss History

In the past 3 years, has the Applicant proposed for this insurance:

a. Received any complaints or written demands or been a subject in litigation involving matters of privacy, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information? Yes ○ No ○

b. Been the recipient of a government investigation or proceedings regarding any alleged violation of privacy law or regulation? Yes ○ No ○

c. Has the Applicant or a third-party who is responsible for the organizations data, notified customers, clients or any third party of any security breach or privacy breach? Yes ○ No ○

d. Been subjected to any cyber extortion demand or threat? Yes ○ No ○

e. Sustained any unscheduled network outage? Yes ○ No ○

f. Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud? Yes ○ No ○

If the Applicant has selected Yes for any of the above Loss History questions, please provide full information including a description of the event, how you responded, the incurred financial loss to your organization, whether the incident is considered remediated or open/ closed if cyber insurance is currently purchased.

Enter Here

Measured
Trust, quantified.

Does the Applicant proposed for this insurance have knowledge of any security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim?

Yes ○
No ○

If 'Yes' to any of the above, please provide details regarding such incident(s) or event(s):

Enter Here

By completing this application, you attest to the best of your knowledge that the controls and security measures are accurate and may be questioned/validated by Measured at any time.

Sign & Date

Contact Name Enter Here

Title Enter Here

Contact Email Enter Here

Applicant Signature

Date

Please return this completed form to your broker. If you have any questions, or don't have an insurance broker, please contact us at: info@measuredinsurance.com

Measured
Trust, quantified.

Authorization Notice

The undersigned authorized officer, owner or manager of the Applicant hereby acknowledges that he/she is aware that the limit of liability contained in the Cyber Coverage Part shall be reduced, and may be completely exhausted, by the costs of legal defense and, in such event, the insurer shall not be liable for the costs of legal defense or for the amount of any judgment or settlement to the extent that such exceeds the limit of liability of the Cyber Coverage Part.

The undersigned authorized officer, owner or manager of the Applicant hereby acknowledges that he/she is aware that legal defense costs that are incurred shall be applied against the deductible amount.

The undersigned authorized officer, owner or manager of the applicant declares that the information furnished in this application is complete, true and correct. The undersigned authorized officer, owner or manager agrees that if the information supplied on this application changes between the date of this application and the effective date of the insurance, he/she (undersigned) will, in order for the information to be accurate on the effective date of the insurance, immediately notify the insurer of such changes, and the insurer may withdraw or modify any outstanding quotations and/or authorizations or agreements to bind the insurance.

The submission of this Application does not bind the Applicant or the insurer to complete the issuance of insurance, but it is agreed that the statements contained in this Application and any other information and/or materials submitted to the insurer in connection with the underwriting of this insurance are the basis of the contract should a policy be issued, and have been relied upon by the insurer in issuing any policy.

This Application and all information and materials submitted with it shall be deemed attached to and become part of the policy if issued. The information contained in the Application shall be deemed material to the insurer's decision to issue any policy.

Any intentional or negligent misrepresentation, omission, concealment or incorrect statement of a material fact, in this application or otherwise, shall be grounds for the rescission** of any bond or policy issued.

For Maine and Maryland Applicants Only: The word "rescission" in the above is deleted and replaced with "denial".

For Georgia Applicants Only: Any misrepresentation, omission, concealment or incorrect statement of a material fact, in this application or otherwise, shall be grounds for denying coverage and cancelling any bond or policy issued.

For Louisiana Applications Only: Any misrepresentation, omission, concealment or incorrect statement of a material fact, in this application or otherwise, shall be grounds for the denial of any claim related to any such misrepresentation, omission, concealment or incorrect statement or the cancellation of any bond or policy issued, provided that coverage will continue for legitimate claims until the cancellation is effective.

Signing of this application does not bind the applicant or the insurer to complete the insurance, but it is agreed that this application shall be the basis of the contract should a cyber coverage part be issued

For Utah Applicants Only: The application and all relevant documents will be attached to the policy at the time of delivery.

Fraud Warnings

To All Prospective Insureds: Any person who knowingly, and with intent to defraud any insurance company or other person, files an application for insurance or statement of claim containing any materially false information, or, for the purpose of misleading, conceals information concerning any fact material thereto, may commit a fraudulent insurance act which is a crime and subjects such person to criminal and civil penalties in many states.

To Prospective Insureds In: Notice to Alabama, Arkansas, District of Columbia, Louisiana, New Mexico, Rhode Island, and West Virginia Applicants: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Colorado Applicants: It is unlawful to knowingly provide false, incomplete or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claiming with regard to a settlement or award payable for insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

Notice to Florida Applicants: Any person who knowingly and with intent to injure, defraud or deceive any insurance company, files a statement of claim containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Notice to Kansas Applicants: An act committed by any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto.

Notice to Kentucky and Pennsylvania Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for

(Fraud Warnings continued on next page)

Fraud Warnings (cont.)

insurance or statement of claim containing any materially false information or conceals for purposes of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

Notice to Maine, Tennessee, Virginia and Washington Applications: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines and/or denial of insurance benefits.

Notice to Maryland Applicants: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Minnesota Applicants: A person who files a claim with intent to defraud or helps commit a fraud against an insurer is guilty of a crime.

Notice to New Hampshire Applicants: Any person who, with a purpose to injure, defraud or deceive an insurance company, files a statement of claim containing any false, incomplete or misleading information is subject to prosecution and punishment for insurance fraud as provided in RSA 638:20.

Notice to New Jersey Applicants: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Notice to New York Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime, and shall also be subject to a civil penalty not to exceed $5,000 and the stated value of the claim for each such violation.

Notice to Ohio Applicants: Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

Notice to Oklahoma Applicants: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, files a statement of claim containing any false, incomplete or misleading information is guilty of a felony.

Notice to Oregon Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or, conceals, for the purpose of misleading, information concerning any fact material thereto, may be guilty of a fraudulent act, which may be a crime and may subject such person to criminal and civil penalties.

Notice to Vermont Applicants: Any person who knowingly presents a false statement in an application for insurance may be guilty of a criminal offense and subject to penalties under state law.