Harris Global Insurance

CYBER LIABILITY APPLICATION FORM

Note: This Application Form must be completed by the Proposed Insured.

1. INSUREDS NAME & MAILING ADDRESS:

Applicants Company Name:	

Applicants Mailing Address:	
	Zip (postcode):

Website Address:	**www.**

2. BUSINESS ESTABLISHED:

Year Business Established:	

3. DESCRIPTION OF INSUREDS BUSINESS OPERATIONS

Business Activities:	

4. ANNUAL REVENUE:

Last Complete Financial Year Revenue:	**$**

Harris Global Insurance

5. COVERAGE REQUIRED:

Please indicate which limit options you would like to receive a quotation for:

Cyber Incident Response:	**$250k ☐**	**$500k ☐**	**$1m ☐**	**$5m ☐**
Cyber & Privacy Liability:	**$250k ☐**	**$500k ☐**	**$1m ☐**	**$5m ☐**
System Damage & Business Interruption:	**$250k ☐**	**$500k ☐**	**$1m ☐**	**$5m ☐**
Cyber Crime:	**$100k ☐**	**$250k ☐**	**$1m ☐**	

6. PREVIOUS CYBER INCIDENTS:

Please tick all the boxes below that relate to any cyber incidents that you have experienced in the last three years (there is no need to highlight events that were successfully blocked by security measures):

☐ Cyber Crime	**☐ Cyber Extortion**	**☐ Data Loss**	**☐ Denial of Service Attack**
☐ IP Infringement	**☐ Malware Infection**	**☐ Privacy Breach**	**☐ Ransomware**
☐ Other			

** If you have ticked any of the boxes, did the incident (s) have a direct financial impact upon your business of more than $10,000 ☐ Yes ☐ No

If yes please provide more information below, including details of the financial impact and measures taken to prevent the incident from occurring again:

_____

_____

Harris Global Insurance

7. COMPANY INFORMATION:

What was your approximate operational expenditure on IT security in the last financial year (including salaries, annual licenses, consultancy costs etc.):	**$**
What was your approximate capital expenditure on IT security in the last financial year (including hardware, one off software costs, etc.):	**$**
Do you anticipate spending more, the same or less in this financial year?	**☐ More** **☐ Less**
Is your IT infrastructure primarily operated and managed in-house or outsourced? **If it is outsourced, who do you outsource it to? _____**	**☐ In-house** **☐ Outsourced**
How many full-time employees do you have in your IT department?	
How many of these employees are dedicated to a role in IT security?	

8. INFORMATION SECURITY GOVERNANCE

Who is responsible for IT security within your organization (by job title)?	
How many years have they been in this position within your company?	
Do you comply with any internationally recognized standards for information governance? **If yes which ones:**	**☐ Yes ☐ No** **_____** **_____**

Harris Global Insurance

9. CLOUD SERVICE PROVIDERS:

Please tick all boxes below that relate to companies or services where you store sensitive data or who you rely upon to provide critical business services:

☐ Adobe	☐ Amazon Web Services	☐ Dropbox	☐ Google Cloud
☐ IBM	☐ Microsoft 365	☐ Microsoft Azure	☐ Oracle Cloud
☐ Rackspace	☐ Salesforce	☐ SAP	☐ Workday

10. CYBER SECURITY CONTROLS

Please tick all the boxes that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you are unsure of what any of theses tools are, please refer to the explanations on the final page of this document:

☐ Advanced Endpoint Protection	☐ Application Whitelisting	☐ Asset Inventory
☐ Custom Threat Intelligence	☐ Database Encryption	☐ Data Loss Prevention
☐ Intrusion Detection System	☐ DMARC	☐ DNS Filtering
☐ Employee Awareness Training	☐ Incident Response Plan	☐ DDoS Mitigation
☐ Mobile Device Encryption	☐ Penetration Tests	☐ Perimeter Firewalls
☐ Security Info & Event Management	☐ Two-Factor Authentication	☐ Vulnerable Scans
☐ Web Application Firewall	☐ Web Content Filtering	

Please provide the name of the software or service provider that you use for each of the controls highlighted above:

_____

_____

_____

Should there not be enough room on this application form to fully enter the details required, please continue on a separate sheet of paper and attach to this application form.

IT IS THE DUTY OF THE INSURED AND THE INSURED'S AGENT TO DISCLOSE ALL MATERIAL FACTS TO UNDERWRITERS BEFORE THE CONTRACT OF INSURANCE IS CONCLUDED AND ANY FAILURE TO DO SO MAY VOID THE INSURANCE CONTRACT. COMPLETION OF THIS QUESTIONNAIRE DOES NOT RELIEVE THE INSURED AND THEIR AGENTS OF THIS DUTY AND IT IS ESSENTIAL THAT ALL MATERIAL FACTS WHICH ARE NOT INCLUDED WITHIN THE ANSWERS TO THE QUESTIONS POSED HEREIN ARE DISCLOSED TO UNDERWRITERS IN ADDITION.

I (THE APPLICANT) DECLARE THAT THE ATTACHED PARTICULARS AND ANSWERS ARE TRUE, CORRECT AND COMPLETE IN EVERY RESPECT TO MY KNOWLEDGE AND BELIEF. I AGREE THAT THIS APPLICATION AND DECLARATION SHALL FORM THE BASIS OF INSURANCE BETWEEN ME AND THE UNDERWRITERS IF A POLICY IS ISSUED.

Name and Position: _____

Signed: _____ **Dated: _____**

Harris Global Insurance

CYBER SECURITY CONTROLS EXPLAINED

Advanced endpoint protection

Software installed on individual computers (endpoints) that uses behavioural and signature based analysis to identify and stop malware infections.

Application whitelisting

A security solution that allows organizations to specify what software is allowed to run on their systems, in order to prevent any non-whitelisted processes or applications from running.

Asset inventory

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices

Custom threat intelligence

The collection and analysis of data from open source intelligence (OSINT) and dark web sources with intelligence on cyber threats and cyber threat actors pertinent to them.

Database encryption

Where sensitive data is encrypted whilst it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss prevention

Software that can identify if sensitive data is exfiltrated from a network or computer system.

DDoS mitigation

Hardware or cloud based solutions used to filter out malicious traffic associated with a DDoS attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC

An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering

A specific technique to block access to known bad IP addresses by users on your network.

Employee awareness

Training programmes designed to increase employee's security awareness. For example, programmes can focus on how to identify potential phishing emails.

Incident response plan

Action plans for dealing with cyber incidents to help guide an organization's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Mobile device encryption

Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Penetration tests

Authorized simulated attacks against an organization to test its cyber security devices. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls

Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Security info & event management (SIEM)

System used to aggregate, correlate and analyse network security information – including messages, logs and alerts – generated by different security solutions across a network.

Two-factor authentication

Where a user authenticates themselves through two different means when remotely logging into a computer system or web-based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Vulnerability scans

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall

Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

We content filtering

The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organization. For example, known malicious websites are typically blocked through some form of web content filtering.