AXIS CYBER RANSOMWARE SUPPLEMENTAL APPLICATION

AXIS INSURANCE
111 S. Wacker Dr., Ste. 3500
Chicago, IL 60606
Telephone**: (678) 746-9000** | Toll-Free**: (866) 259-5435** | Fax: **(678) 746-9315**
https://www.axiscapital.com/insurance/cyber-technology-e-o

SOLELY AS RESPECTS CLAIMS-MADE LIABILITY COVERAGES UNDER THE POLICY FOR WHICH THIS APPLICATION IS BEING SUBMITTED: THIS INSURANCE POLICY PROVIDES COVERAGE ON A CLAIMS-MADE AND REPORTED BASIS AND APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR ANY APPLICABLE EXTENDED REPORTING PERIOD AND REPORTED TO THE INSURER AS SET FORTH IN THE REPORTING OF CLAIMS AND EVENTS SECTION. DEFENSE COSTS ARE INCLUDED IN THE LIMITS OF INSURANCE, AND PAYMENT THEREOF WILL ERODE, AND MAY EXHAUST, THE LIMITS OF INSURANCE.

ABOUT THIS APPLICATION

- "Applicant" refers individually and collectively to all proposed insureds. All responses shall be deemed made on behalf of all proposed insureds. **If responses differ for any proposed insureds (including subsidiaries) please complete additional supplementals for those.**
- This Application and all materials submitted herewith shall be held in confidence.
- The submission of this Application does not obligate the Applicant to buy insurance nor is the Insurer obligated to sell insurance or to offer insurance upon any specific terms requested.
- If the policy applied for is issued, this Application, which shall include all Supplemental Applications and material and information submitted in connection with this Application, will be deemed attached to and will form a part of the policy.

INSTRUCTIONS

Respond to all questions completely, leaving no blanks. Check responses when requested.

If space is insufficient, continue responses in additional commentary box at the end of the supplemental.

This Application must be completed, dated, and signed by an authorized officer of the entity identified in the section entitled "Applicant Information" on the main Application.

RANSOMWARE SUPPLEMENT

Applicant Name & Mailing Address:	Test Company Axis Application

AXIS CYBER RANSOMWARE SUPPLEMENTAL APPLICATION

Governance & Controls:	Does the Applicant employ any intrusion detection and prevention solution?	☑ Yes ☐ No
Does the Applicant employ an endpoint detection and response solution (EDR)?		☑ Yes ☐ No
If yes, what % of the Applicant's endpoints is EDR deployed on?		95 %
If yes, what % of the Applicant's servers is EDR deployed on?		80 %
Please identify EDR solution(s) in place, including company names & product name:	Windows Defender	
Does the Applicant employ Microsoft (Office) 365?		☐ Yes ☑ No
If yes, are the following implemented?		
Microsoft 365 Advanced Threat Protection (ATP)/Defender ☐ Yes ☐ No	Multi Factor Authentication for all Microsoft 365 users ☐ Yes ☐ No	

Is Multi Factor Authentication required for the following access?				
Remote access ☑ Yes ☐ No	Critical Information ☑ Yes ☐ No	Personal devices ☑ Yes ☐ No	Third Party/Vendor Access ☑ Yes ☐ No	Noncritical information and applications ☑ Yes ☐ No

Does the Applicant utilize a Privileged Access Management (PAM) tool?	☑ Yes ☐ No
If yes, is access to the PAM tool subject to Multi Factor Authentication?	☑ Yes ☐ No
If no, please describe how the Applicant is securing privileged and administrator accounts:	

What secondary factor method is the Applicant using for Multi Factor Authentication?	SMS ☑ Yes ☐ No
	Non-Corporate Device (if Yes above) ☐ Yes ☑ No

Biometric Authentication ☐ Yes ☑ No	Authenticator Application ☐ Yes ☑ No	Secondary Email ☐ Yes ☑ No	Endpoint Certificate ☐ Yes ☑ No	Physical Security Keys ☐ Yes ☑ No

Identify any other:	
Please identify the number of domain and service accounts the Applicant has in the Domain Admin Group: 5	

Are these stored in either of the following?	Local Directory ☐ Yes ☑ No	Active Directory ☐ Yes ☑ No

Identify any other:				
Does the Applicant employ any of the following solutions?	SPF ☑ Yes ☐ No	DKIM ☑ Yes ☐ No	DMARC ☑ Yes ☐ No	
Does the Applicant actively monitor all administrator access for unusual behavior patterns?	☑ Yes ☐ No			
Is Remote Desktop Protocol (RDP) enabled?	☐ Yes ☑ No			
If yes, is RDP accessible:	Internally ☑ Yes ☐ No	Externally ☐ Yes ☑ No		
Are the following implemented?				
VPN access with Multi Factor Authentication only ☑ Yes ☐ No	Multi Factor Authentication for access ☑ Yes ☐ No	Accessed through PAM? ☐ Yes ☑ No	Network level authentication enabled ☐ Yes ☑ No	
Identify any other controls/securities in place for RDP usage:				
Please give an overview of the Applicant's vulnerability management and critical patching process & timeline if outside of the below:				
Critical patching target:	☑ < 24 Hours	☑ 24-72 Hours	☐ 3-7 days	☐ > 7 Days
Normal Vulnerability Management patching target:	☐ < 7 Days	☐ 7-14 Days	☑ 14-30 Days	☐ > 30 Days
Does the Applicant have a Security Operations Center (SOC)?	☐ Yes ☑ No			
If yes:	Is it monitored 24/7? ☐ Yes ☐ No	Is it managed internally or by a third party?		
		Internally ☐ Yes ☐ No	Third Party ☐ Yes ☐ No	Hybrid ☐ Yes ☐ No
Any other information on the Applicant's SOC:				

If the Applicant has any End-of-Life software or systems in their environment, please give an overview of usage, remediation plans, decommission strategy, segregation and any other additional controls or securities in place to secure:	none	
Has the Applicant applied network segmentation within their environment?		☑ Yes ☐ No
If yes, please indicate on what basis:	Geography ☐ Yes ☑ No	System Criticality ☑ Yes ☐ No
	Subsidiaries ☐ Yes ☐ No	Brick and Mortar Locations ☐ Yes ☐ No
	Business Function ☐ Yes ☑ No	Data Classification ☐ Yes ☐ No
Any other Network Segmentation details/points to clarify:		

Training & Awareness:	Does the Applicant conduct mandatory information security and privacy training of employees and contractors having the following content at least annually?				
Social engineering ☑ Yes ☐ No	Phishing campaigns ☑ Yes ☐ No		Role based training ☑ Yes ☐ No		
Security/threat awareness ☑ Yes ☐ No	Privacy/data handling compliance ☐ Yes ☑ No		Identify any other:		
Are Phishing Simulations conducted for all employees?					☑ Yes ☐ No
How frequently is the Applicant conducting Phishing Simulations?		☐ Monthly	☐ Quarterly	☑ Semi annually	☐ Annually
Are Phishing Simulations:	Role Based ☑ Yes ☐ No	Targeted ☑ Yes ☐ No	Sent in a staggered fashion ☐ Yes ☑ No		
Click Rate of most recent simulation		☐ < 5%	☑ 5-10%	☐ 10-15%	☐ 15-20%	☐ > 20%
Reporting Rate of most recent simulation:		☐ < 5%	☐ 5-10%	☑ 10-15%	☐ 15-20%	☐ > 20%
Does the Applicant have a report phishing email add-in enabled for all email users?					☑ Yes ☐ No
Does the Applicant employ a sandboxing solution for investigating suspicious emails/attachments?					☑ Yes ☐ No
How does the Applicant handle repeat offenders/clickers?					

AXIS CYBER RANSOMWARE SUPPLEMENTAL APPLICATION

Backups:	Does the Applicant conduct regular back up of data?			☑ Yes ☐ No
How frequently is Critical Information backed up? At least:			☐ Continuously	☑ Daily
☐ Weekly	☐ Monthly	☐ Quarterly	☐ Semi annually	☐ Annually
Which of the following does the Applicant utilize for backups?		Tapes ☑ Yes ☐ No	Disks ☐ Yes ☐ No	Cloud ☐ Yes ☐ No
Where are backups stored? Select all that apply			MSSP ☑ Yes ☐ No	On premises ☑ Yes ☐ No
Offline storage ☑ Yes ☐ No	Offsite storage ☐ Yes ☐ No		Secondary data center ☐ Yes ☐ No	
Please give an overview of the Applicant's backup strategy and who has access to the backup environment:				

Are backups subject to the following measures?					
Multi Factor Authentication ☑ Yes ☐ No	Encryption ☑ Yes ☐ No	Segmentation ☑ Yes ☐ No	Virus/malware scanning ☐ Yes ☐ No	Immutable ☑ Yes ☐ No	Privileged Access Management ☐ Yes ☐ No
Identify any additional securities/controls:					

Unique backup credentials stored separately from other user credentials				☑ Yes ☐ No
If backups are encrypted, are encryption keys stored offline?				☑ Yes ☐ No
How frequently are backups made to offsite storage? At least:	☐ Daily	☐ Weekly	☐ Monthly	☐ Quarterly
How frequently are backups made to offline storage? At least:	☑ Daily	☐ Weekly	☐ Monthly	☐ Quarterly
How frequently is a full recovery from a backup tested? At least:		☐ Monthly	☐ Quarterly	☑ Annually

Recovery Time & Impact:	In the event of an interruption of the Applicant's network, what is the Applicant's recovery time objective for critical systems, applications and processes? At most:			
☐ < 8 hours	☐ 8-12 hours	☑ 12-24 hours	☐ 24-48 hours	☐ > 48 hours
Have these been validated in the last 12 months?				☐ Yes ☐ No
In the event Critical Information, or critical systems, applications or processes became unavailable, how long would it take to materially interrupt the Applicant's business? At most:				
☐ < 1 hour	☑ 1-8 hours	☐ 8-12 hours	☐ 12-24 hours	☐ 24-48 hours

Any Additional Comments:	

REPRESENTATIONS AND SIGNATURE

By signing this document, the undersigned authorized representative of the Applicant represents on behalf of all persons and entities proposed for coverage, after inquiry, that to the best of their knowledge:

1. The statements and answers given in and all materials submitted with this Application are true, accurate and complete.
2. No facts or information material to the risk proposed for insurance have been misstated or concealed.
3. These representations are a material inducement to the Insurer to provide a proposal for insurance.
4. Any policy the Insurer issues will be issued in reliance upon these representations.
5. The Applicant will report to the Insurer immediately in writing any material change in the Applicant's activities, products and services.
6. The Applicant will report to the Insurer immediately in writing any material changes to the answers provided in this Application which occur or are discovered between the date of this Application and the effective date of the policy for which coverage is sought by submission this Application.
7. The Insurer reserves the right, upon receipt of any such notice, to modify or withdraw any proposal for insurance the Insurer has offered.

WARNING

PLEASE REVIEW THE STATE FRAUD STATEMENT CONTAINED AT THE END OF THIS APPLICATION APPLICABLE TO THE STATE IN WHICH THE APPLICANT RESIDES.

Any person who, with intent to defraud or knowingly facilitates a fraud against the insurer, submits an application or files a claim containing a false or deceptive statement may be guilty of insurance fraud.

This Application must be signed by the Applicant's Chief Executive Officer, President, Chief Information Officer, Chief Technology Officer, Chief Security Officer, Chief Operating Officer, Chief Financial Officer or General Counsel or Risk Manager, or their functional equivalent, unless the Insurer instructs the Applicant otherwise.

Name _____ Name (Signature) _____

Title _____

Date _____

TO BE COMPLETED BY PRODUCERS ONLY:

RETAIL PRODUCER		WHOLESALE PRODUCER	
Producer Name: **City, State:** **Telephone No.:** **License No.:**		**Producer Name:** **City, State:** **Telephone No.:** **License No.:**	

Producer Signature: _____

STATE FRAUD STATEMENT

ALABAMA

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to restitution fines or confinement in prison or any combination thereof.

ARKANSAS

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.

CALIFORNIA

For your protection, California law requires the following warning to appear on this form: Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

COLORADO

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 claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado division of insurance within the department of regulatory agencies.

DISTRICT OF COLUMBIA

Warning: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits if false information materially related to a claim was provided by the applicant.

FLORIDA

Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete or misleading information is guilty of a felony of the third degree.

KANSAS

A “fraudulent insurance act” means 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 electronic, electronic impulse, facsimile, magnetic, oral, or telephonic communication or 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.

KENTUCKY

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance 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.

LOUISIANA

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.

MAINE

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 or a denial of insurance benefits.

MARYLAND

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.

NEW JERSEY

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

NEW MEXICO

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 civil fines and criminal penalties.

NEW YORK

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 five thousand dollars and the stated value of the claim for each such violation.

OHIO

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.

OKLAHOMA

WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

OREGON

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

In order for us to deny a claim on the basis of misstatements, misrepresentations, omissions or concealments on your part, we must show that:

A. The misinformation is material to the content of the policy;

B. We relied upon the misinformation; and

C. The information was either:

   1. Material to the risk assumed by us; or

   2. Provided fraudulently.

For remedies other than the denial of a claim, misstatements, misrepresentations, omissions or concealments on your part must either be fraudulent or material to our interests.

With regard to fire insurance, in order to trigger the right to remedy, material misrepresentations must be willful or intentional. Misstatements, misrepresentations, omissions or concealments on your part are not fraudulent unless they are made with the intent to knowingly defraud.

PENNSYLVANIA

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 subjects such person to criminal and civil penalties.

PUERTO RICO

Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand dollars ($5,000) and not more than ten thousand dollars ($10,000), or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances be present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

RHODE ISLAND

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.

TENNESSEE

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

VERMONT

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.

VIRGINIA

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

WASHINGTON

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

WEST VIRGINIA

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.