NETGUARD® PLUS
CYBER LIABILITY
FOR SMALL MUNICIPALITIES

Minnesota Service Cooperative
NetGuard® Plus Cyber Liability Program
For Small Municipalities

The Minnesota Service Cooperatives have partnered with Hausmann-Johnson Insurance and NAS Insurance Services to offer a streamlined NetGuard**®** Plus Cyber Liability Insurance application process and simplified underwriting for small municipalities that meet program qualifications. Applicants can simply complete the Program Application, request to bind coverage, and pay the applicable premium.

COVERAGE COMPONENTS

- **Multimedia Liability** – Duty to defend coverage for third party claims alleging liability resulting from the dissemination of online or offline media material, including claims alleging copyright/trademark infringement, libel, slander, plagiarism or personal injury.

- **Security and Privacy Liability** – Duty to defend coverage for third party claims alleging liability resulting from a security breach or privacy breach, including failure to safeguard electronic or non-electronic confidential information; failure to prevent virus attacks; denial of service attacks; the transmission of malicious code from an insured computer system to the computer system of a third party; or acts committed by rogue employees.

- **Privacy Regulatory Defense and Penalties** - Duty to defend coverage for regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, or local governmental agencies, such as proceedings/investigations alleging HIPAA violations.

- **Breach Event Costs** – Coverage for reasonable and necessary mitigation costs and expenses incurred as a result of a privacy breach, security breach or adverse media report, including legal expenses, public relations expenses, advertising and IT forensic expenses, postage, and the cost to provide call centers, credit monitoring and identity theft assistance.

- **Proactive Privacy Breach Response Costs (sub-limit of Breach Event Costs)** - Coverage for public relations expenses incurred in response to a security breach or privacy breach, but prior to the publication of an adverse media report, in an effort to avert or mitigate reputational harm which could result from the adverse media report.

- **Voluntary Customer Notification Expenses (sub-limit of Breach Event Costs)** - Coverage for expenses incurred in notifying parties of a privacy breach where there is no requirement by law to do so.

- **BrandGuard®** - Coverage for loss of net profit incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach.

- **Network Asset Protection** – Coverage for reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased or corrupted due to (1) accidental damage or destruction of electronic media or computer hardware, (2) administrative or operational mistakes in the handling of electronic data, or (3) computer crime/attacks including malicious code and denial of service attacks. Coverage also extends to business income loss and

interruption expenses incurred because of a total or partial interruption of an insured computer system directly caused by any of the above events.

- **Cyber Extortion** – Coverage for extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.

- **Cyber Crime** – Coverage for loss of money or securities incurred due to financial fraud, including wire transfer fraud; charges incurred for unauthorized calls resulting from fraudulent use of an insured telephone system; expenses incurred to notify customers of phishing schemes that impersonate the Insured or the Insured's brands, products or services, and the costs of reimbursing customers for losses resulting from such phishing schemes.

- **PCI DSS Liability** - Duty to defend coverage for assessments, fines, or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.

PROGRAM HIGHLIGHTS

- Broad coverage for data that is stored with third parties, including BPO service providers, outsourced IT providers and independent contractors
- Expanded Cyber Crime coverage; expanded to include loss of money AND other property
- Separate Breach Event Costs Limit - $1M limit
- Separate Claim Expenses Limit - $1M limit
- Worldwide coverage - claims can be brought outside of the U.S.
- Network Asset Protection coverage triggers include accidental damage or destruction, administrative and operational mistakes as well as computer crimes, including acts of cyber terrorism
- Blanket Dependent Business Interruption coverage under Network Asset Protection - $1M limit
- TCPA Defense Costs Sublimit - $75,000 limit
- ADA Non-Compliance Costs Sublimit - $25,000 limit
- Court Attendance Costs Sublimit - $50,000 limit
- Reward Expenses Sublimit - $100,000 limit
- Property Damage exclusion does not apply to electronic data
- Includes coverage for breach of corporate information
- Acts committed by rogue employees are covered, as well as privacy claims brought by employees
- Multimedia Liability and Security & Privacy Liability include coverage for liability assumed under contract
- Extended Reporting Period available for 1-3 years

PROGRAM QUALIFICATIONS

☐ Must not have experienced any privacy or security claims/incidents in the past 5 years.

☐ Must have a firewall and anti-virus system in place.

☐ Must be a current member of a Minnesota Service Cooperative.

☐ Must be a municipality with a population of 50,000 or less.
(Larger risks can be submitted to NAS for further consideration)

Coverage cannot be bound under the terms and conditions of this program for Applicants that do not fall within the program qualifications; however, Applicants may be considered for coverage outside of the program, subject to underwriting review.

Hausmann | Johnson
INSURANCE

The Minnesota
Service Cooperatives

NAS

LIMITS

Limits are subject to and in excess of a self insured retention. Higher limit options available by request.

I.	Multimedia Liability	$1,000,000
II.	Security and Privacy Liability	$1,000,000
III.	Privacy Regulatory Defense and Penalties	$1,000,000
IV.	Breach Events Costs	$1,000,000
	Proactive Privacy Breach Response Costs Sublimit	$ 25,000
	Voluntary Notification Expenses Sublimit	$1,000,000
V.	BrandGuard®	$1,000,000
	Waiting period	**2 weeks**
	Period of Indemnity	**6 months**
VI.	Network Asset Protection	$1,000,000
	Digital Assets Loss/Special Expenses	
	Non-Physical Business Interruption/Extra Expense	
	Waiting Period (applicable to business interruption)	**4 hours**
VII.	Cyber Extortion	$1,000,000
VIII.	Cyber Crime	$125,000*
IX.	PCI DSS Liability	$1,000,000
	Maximum Policy Aggregate Limit of Liability:	$1,000,000

* Cyber Crime $250,000 limit option available for an additional premium of 7.5%

RISK MANAGEMENT WEBSITE ACCESS

POLICY & ENDORSEMENT LINKS

Rates apply to the NetGuard® Plus Program, written by NAS on NetGuard® Plus Policy Form **P1856NGP-0416** and endorsed with:

- Nuclear Incident Exclusion Clause (E1856A-0710)
- U.S. Treasury Department's Office of Foreign Assets Control (OFAC) Advisory Notice to Policyholders (E1856US-0315)
- Breach Event Costs Outside Limits (E1856NM-0416)
- Dependent Business Interruption Blanket Sublimit (E1856NES-0117) – 12 hour waiting period
- Minnesota Service Cooperative Cyber Amendatory (E1856NHG-0118)
- Minnesota Service Cooperative Coverage Enhancements (E1856NHH-0118)

HOW TO PURCHASE THIS INSURANCE

1. Log onto www.hausmann-johnson.com/msccyber to complete a brief online application.

2. Within three business days, you will receive an email from cyber@hausmann-johnson.com with your final premium confirmation. Please be sure to whitelist this email address.

3. Simply reply to the premium confirmation email confirming that you would like to bind coverage. Your policy and invoice will then be available to you through an online portal. Details about how to access the portal will be communicated after coverage has been bound.

CYBER RISK SCENARIOS

Security and Privacy Liability

A laptop belonging to the IT Director of a school district was stolen from the IT Director's car while it was parked in the school's parking lot. The laptop contained the personal information of students, including contact information and social security numbers.

The IT Director did not take precautions to encrypt or otherwise protect the data on his laptop, which was a violation of the school district's privacy policy.

The school district reported the lost laptop to local law enforcement and notified the families of affected students. Several families filed a class action lawsuit against the school district for failure to safeguard the students' private information. The school district's cyber insurance covered defense costs and damages awarded against the school district.

Cyber Crime

An accountant at a small municipality in Chicago received an e-mail from a member of the municipality's finance committee requesting a wire transfer be processed in the amount of $50,000.

The wire was sent, but, in a later conversation with the head of the finance committee, the accountant discovered that the committee had not actually requested the wire transfer. In fact, the e-mail the accountant received was a "spoof" e-mail, sent by a hacker who had created a fraudulent e-mail account to impersonate a finance committee member.

The bank would not return the municipality's funds because the transfer appeared to be legitimate. The municipality was reimbursed for the financial loss under Cyber Crime insurance.

Breach Event Costs

An iPad issued to a city hall employee went missing. The iPad contained confidential records, including personally identifiable information (PII) of over 1,000 residents of the municipality. The Insured's cyber insurance reimbursed the Insured for the costs incurred to notify affected residents of the breach and for costs associated with 12 months of credit monitoring.

APPLICATION for: **NetGuard® Plus Minnesota Service Cooperative Cyber Program**

Claims Made Basis. Underwritten by Underwriters at Lloyd's, London

Notice: The Policy for which this Application is made applies only to Claims made against any of the Insureds during the Policy Period. The Limit of Liability available to pay damages or settlements shall be reduced and may be completely exhausted by amounts incurred as defense costs. Defense costs shall be applied to the retentions. Submission of this Application does not guarantee coverage.

General instructions for completing this Application:

1. **Please read carefully and answer all questions. If a question is not applicable, so state by writing "Not Applicable".**

2. **The completed Application should include all information relative to all subsidiaries and locations to be covered.**

3. **The Application must be signed by an executive officer.**

4. **Please read the Policy for which application is made (the "Policy") prior to completing this Application. The terms as used herein shall have meanings as defined in the Policy.**

SECTION I.   YOUR DETAILS

1. Name of Applicant: _____
    (Include names of all subsidiaries or affiliated companies to be insured; attach a separate sheet, if necessary)

    Applicant Type: ☐ Individual   ☐ Corporation   ☐ Partnership   ☐ Other

    Headquarters Address: _____

    Mailing Address *(if different)*: _____

    Telephone Number: _____   Fax Number: _____

    Email Address: _____

    Corporate Website Address: _____

    Nature of Business: _____

SECTION II. YOUR BUSINESS

2. Date established: _____

3. Are any significant changes in nature or size (e.g., more than 20% increase in revenue) of Applicant's business anticipated over the next twelve (12) months?   ☐ Yes ☐ No
    If "Yes", please explain: _____

SECTION III.   EXPOSURE INFORMATION

ANNUAL BUDGET AND EXPOSURE BASE

4.   Total Annual Budget: $ _____   Current population: _____

5.   Please estimate the total number of customer and employee records you store either electronically or in physical files.

Current number: _____   For the Next 12 Months: _____

6.   Please estimate the total number of credit card transactions for the next 12 months: _____

SECTION IV.   NETWORK SECURITY AND PRIVACY

7.	Do you enforce a security policy that must be followed by all employees, contractors, or any other person with access to your network?	☐ Yes ☐ No
8.	Does your security and privacy policy include mandatory training for all employees?	☐ Yes ☐ No
9.	If required by law, are you HIPAA compliant? ☐ Yes	☐ No ☐ N/A
10.	Do you process, store, or handle credit card transactions?	☐ Yes ☐ No
	If "**Yes**", are you PCI-DSS Compliant at the time of application?	☐ Yes ☐ No
11.	Has the Applicant or any other organization proposed for this insurance experienced a wire transfer, telecom fraud or phishing attack loss in the past five years?	☐ Yes ☐ No
	If "**Yes**", please provide complete details, including information on any remediating steps that have been implemented._____	
12.	Does the Applicant utilize a cloud provider to store data?	☐ Yes ☐ No
	If "**Yes**", please list the name of the cloud provider: _____	
	If more than one provider is utilized, please list the provider that stores the most confidential information for the Applicant.	
13.	Does your virus or malicious code control program address the following: anti-virus on all systems, filtering of all content for malicious code, controls on shared drives and folders, CERT or similar vendor neutral threat notification services, removal of spyware and similar parasitic code?	☐ Yes ☐ No
14.	Do you have a firewall in place?	☐ Yes ☐ No
	If "**Yes**", are your firewalls, information systems and security mechanisms securely configured?	☐ Yes ☐ No
	Check "No" if your systems are configured using factory default settings.	
15.	Do you enforce a software update process that includes monitoring of vendors or automatically receiving notices from them for availability of security patches, upgrades, testing and installing critical security patches?	☐ Yes ☐ No
	If "**Yes**", how frequently is this done? ☐ Weekly ☐ Within 30 days ☐ More than 30 days	
16.	Do you test your security at least yearly to ensure effectiveness of your technical controls as well as your procedures for responding to security incidents (e.g., hacking, viruses, and denial of service attacks)?	☐ Yes ☐ No
	If **"Yes"**, does this include a network penetration test?	☐ Yes ☐ No
17.	Is all sensitive and confidential information that is transmitted within and from your organization encrypted using industry-grade mechanisms?	☐ Yes ☐ No
18.	Is all sensitive and confidential information stored on your organization's databases, servers and data files encrypted?	☐ Yes ☐ No
19.	If encryption is not in place for databases, servers and data files, are the following compensating controls in place:	
	a) Segregation of servers that store confidential information?	☐ Yes ☐ No
	b) Access control with role based assignments?	☐ Yes ☐ No

SECTION V.   LOSS HISTORY

20. Has the Applicant or any other person or organization proposed for this insurance ever received any complaints, claims or been a subject in litigation involving matters of privacy injury, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks, or the Applicant's customers' ability to rely on the Applicant's network?   ☐ Yes ☐ No

    If "Yes", please provide specific details:

21. Do you or any other person or organization 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

22. Has any employee ever been disciplined for mishandling data or otherwise tampering with your computer network?   ☐ Yes ☐ No

    If "Yes", please provide specific details:

23. Has the Applicant or any other organization proposed for this insurance sustained any unscheduled network outage or interruption within the past 24 months?   ☐ Yes ☐ No

    If "Yes", please provide specific details:

SECTION VI.   WARRANTY AND REPRESENTATIONS

1. The undersigned warrants and represents that the statements and information contained in or attached to this Application are true and complete, and that reasonable efforts have been made to obtain sufficient information to facilitate the proper and accurate completion of this Application.

2. Signing of this Application does not bind the undersigned to complete the insurance; however, the Undersigned acknowledges and recognizes that the statements, representations, and information contained in or attached to this Application are material to the risk assumed by the Insurer; that any Policy will have been issued in reliance upon the truth thereof; that this Application shall be the basis of the contract should a Policy be issued; and that this Application, and all information and materials furnished to the Insurer in conjunction with this Application, shall be deemed incorporated into and made a part of the Policy, should a Policy be issued. Underwriters hereby are authorized to make any investigation and inquiry in connection with this Application as they may deem necessary.

3. The undersigned acknowledges and agrees that if the information supplied on this Application or in any attachments changes between the date of the Application and the inception date of the policy period, the Applicant will immediately notify the Insurer of such change, and, the Insurer may withdraw or modify any outstanding quotations and/or agreement to bind the insurance.

4. For purposes of creating a binding contract of insurance by this Application or in determining the rights and obligations under such a contract in any court of law, the parties acknowledge that a signature reproduced by either facsimile or photocopy shall have the same force and effect as an original signature and that the original and any such copies shall be deemed one and the same document.

Signed: _____   Print Name: _____

Title: _____   Date (Mo/Day/Yr): _____

Applicant Organization: _____

SECTION VII.   PAYMENT INSTRUCTIONS

Premium: $ _____

Taxes & Fees: $ _____ *Exact Amount will be confirmed at binding*

Policy Issuance Fee*: $ _____

Broker fee: $ _____

    TOTAL PAYMENT $ _____

*Policy issuance fees vary by state, with $175 being the maximum. NAS will confirm the policy issuance fee at the time of binding.

For risks filed by NAS, please remit all taxes and fees with premium, should coverage be bound with Lloyds through NAS.

- **Policy fee is fully earned.**
- **Written Policies are subject to a minimum earned premium of 25%.**
- **<u>No Flat Cancellations</u>.**