

PO Box 29502 #69121, Las Vegas, Nevada 89126 | P: (858) 618-1648 | F: (858) 618-1655 | [www.cresinsurance.com](http://www.cresinsurance.com)

**Company Name:** \_\_\_\_\_ **DBA:** \_\_\_\_\_

Year Established: \_\_\_\_\_ Subsidiary/Franchise: \_\_\_\_\_

Full Address: \_\_\_\_\_

FEIN: \_\_\_\_\_

**Contact Person:** \_\_\_\_\_

Phone: \_\_\_\_\_ Email: \_\_\_\_\_

**Designated Information Security Contact:** \_\_\_\_\_

Phone: \_\_\_\_\_ Email: \_\_\_\_\_

Title: \_\_\_\_\_ Company: \_\_\_\_\_

**Website and Email Domains (Please add ALL know domains):** \_\_\_\_\_

Primary Industry: \_\_\_\_\_

(ie. Real Estate, Property Management, Mortgage Brokering, Escrow, etc.)

Secondary Industry: \_\_\_\_\_

Total Revenue for the previous 12 months: \_\_\_\_\_

Expected revenue in the next 12 months: \_\_\_\_\_

Number of Employees: \_\_\_\_\_

**Does your organization provide mandatory information security training to all employees at least annually?**

Yes  No

**Does your organization have sensitive information stored on the cloud?**

Yes  No

**Is your organization engaged in any of the following businesses? Select all that apply.**

Adult Content  Cryptocurrency of Blockchain  Gambling  Payment Processing

Managed Service Provider (MSP), Managed Security Service Provider (MSSP), or Remote network administration services provider

None of the above

## CYBER INCIDENT, CLAIM, OR LOSS

During the past three years, did your organization experience a cyber-incident, claim or loss, whether insured or not, which could have been covered under a policy similar to the proposed insurance, this includes but is not limited to any:

- Yes  No Actual or reasonably suspected data breach or security failure, including notifying consumers or third parties of data breach or security failure
- Yes  No Claims or complaints with respect to privacy injury, breach of information or network security, unauthorized disclosure of information, defamation, or content infringement
- Yes  No Government action, investigation, or subpoena regarding any alleged violation of a privacy law or regulation
- Yes  No Actual or attempted extortion demand with respect to its data or computer systems

## POSSIBLE CLAIMS

Does your organization have knowledge or information regarding any fact, circumstance, situation, or event that could reasonably give rise to a claim or loss under the proposed insurance?

- Yes  No

## ENCRYPTION

Does your organization implement encryption on laptop computers, desktop computers, and other portable media devices?

- Yes  No  Sometimes

## PCI, PII, PHI

Does your organization collect, process, store, transmit, or have access to any Payment Card Information (PCI), Personally Identifiable Information (PII), or Protected Health Information (PHI) other than employees of your organization? [What are PII and PHI?](#)

- Yes  No

How many PII or PHI records does your organization collect, process, store, transmit, or have access to?

- Don't Know  None  <100K  100K - 500K  500K - 1M  >1M

What is the estimated annual volume of payment card transactions (credit cards, debit cards, etc.)?

- Don't Know  None  <100K  100K - 500K  500K - 1M  >1M

## CONTENT COMPLAINTS

Within the last 3 years has your organization been subject to any complaints concerning the content of its website, advertising materials, social media, or other publications?

Yes  No

## CONTENT REMOVAL

Does your organization enforce procedures to remove content (including third party content) that may infringe or violate any intellectual property or privacy right?

Yes  No

## WEEKLY BACKUPS

Does your organization maintain at least weekly backups of all sensitive or otherwise critical data and all critical business systems offline or on a separate network?

Yes  No

## MULTI-FACTOR AUTHENTICATION

For which of the following services do you enforce Multi-Factor Authentication (MFA):

Email

Yes  No  N/A - No remote access allowed

Virtual Private Network (VPN)

Yes  No  N/A - No Virtual Private Network allowed

Remote Desktop Protocol (RDP), RDWeb, RD Gateway, or other remote access

Yes  No  N/A - No remote access allowed

Network / cloud administration or other privileged user accounts

Yes  No  On administrative accounts and all cloud services where supported

## FUNDS TRANSFER REQUESTS

Does your organization require a secondary means of communication to validate the authenticity of:

Funds transfer requests (ACH, wire, etc.) before processing a request in excess of \$5000?

Yes  No  N/A

Any request to change banking details (ACH, wire, payroll distribution, etc.)?

Yes  No  N/A

Does the policy holder or their employees verify vendor/supplier bank accounts before adding to their accounts payable systems?

Yes  No  N/A

Does the policy holder or their employees authenticate funds transfer requests (e.g. by calling a customer to verify the request at a predetermined phone number)?

Yes  No  N/A

Does the policy holder or their employees prevent unauthorized employees from initiating wire transfers?

Yes  No  N/A

---

Signature

---

Date