Stateside Underwriting Agency

SUA Cyber Application

335 Commerce Drive, Crystal Lake, IL 60014
Send submissions to submissions@statesideunderwriting.com

Applicant Information

Applicant Name:		
Street Address:	Suite/Unit/Floor #:	
City:	State:	ZIP Code:
Website Address		

Business Information

Complete the following for all Applicants (including subsidiaries) for the preceding 12-month period starting with the month end closest to the date of this Application:

1. a. 12-Month Revenue: $	**b.** 12-Month Loan Origination Volume: $
2. How many records containing personal information do you process or store per year?	

Security and Privacy Controls Information

If you answer "No" to any of the following Questions, please attach an explanation as to each Applicant (including subsidiaries).

3. Do you take full back-ups at least once a week, and with at least one of the following controls in place?		Yes ☐	No ☐
a. Back-up data is stored on a physically disconnected ("air-gapped") device (e.g. tape drive)		Yes ☐	No ☐
b. Access to back-up data requires the use of Multifactor Authentication (MFA)		Yes ☐	No ☐
c. Back-up data is stored in a read-only ("immutable") format		Yes ☐	No ☐
d. Back-up process is automated using a cloud service provider with ransomware protection		Yes ☐	No ☐
4. Have you installed and regularly update anti-malware/ antivirus software on all workstations and servers?		Yes ☐	No ☐
5. Do you change all default passwords on new devices and require regular mandatory password updates for all accounts?		Yes ☐	No ☐
6. Do you have a process in place to regularly patch your systems and applications?		Yes ☐	No ☐
7. Do you configure and use a firewall to protect all your devices, particularly those that connect to public or other untrusted Wi-Fi networks?		Yes ☐	No ☐
8. Do you control access to your data through user accounts, and review who should have administrative access on a regular basis?		Yes ☐	No ☐
9. Do you have a business continuity plan and review such at least annually?		Yes ☐	No ☐
10. If you function in full or part as a manufacturing risk: please confirm that any computer numeric control processes are on a segregated computer system from the rest of the Applicant's systems.	N/A ☐	Yes ☐	No ☐
11. a. Does the applicant have a data retention policy?		Yes ☐	No ☐
b. If so, how long is data retained?			
12. a. Are credit cards or debit cards accepted for payment?		Yes ☐	No ☐
b. If yes, are you PCI compliant?		Yes ☐	No ☐
13. Is Multifactor Authentication (MFA) required for all remote network access and email access?		Yes ☐	No ☐

Heavy Industry Question Set

Only for Applicants in the industries of Manufacturing or utility generation, transmission, distribution, or water or sewage provision

14. If Operational Technology (OT) is used, then both of the following must be true	N/A ☐	Yes ☐	No ☐
a. All connections between IT and OT networks must be segmented using firewalls		Yes ☐	No ☐
b. Multifactor Authentication (MFA) must be enforced for all remote connections to OT networks		Yes ☐	No ☐

For applicants with over $25,000,000 in revenues, please complete the following section

15. Do you conduct annual testing of back-up procedures to ensure that critical data and systems can be restored in the event of a cyber incident?		Yes ☐	No ☐
16. Is mandatory information security training carried out by all employees at least annually?		Yes ☐	No ☐
17. Are all emails scanned for potentially malicious attachments and links?		Yes ☐	No ☐
18. Are critical security patches deployed within 30 days of vendor release?		Yes ☐	No ☐

For applicants with over $50,000,000 in revenues, please complete the following section

19. If end-of-life software is utilized, then at least one of the following must apply:	N/A ☐	Yes ☐	No ☐
a. Confirm devices with end-of-life software installed are not connected to the internet		Yes ☐	No ☐
b. Extended support has been purchased from the vendor for all devices running end-of-life software		Yes ☐	No ☐
20. If applicant stores employee or customer information in cloud applications, confirm MFA is enforced for all login attempts to these applications	N/A ☐	Yes ☐	No ☐
21. If credit or debit card payments are accepted, then both of the following must be true:	N/A ☐	Yes ☐	No ☐
a. Applicant must hold a valid PCI-DSS certificate of compliance		Yes ☐	No ☐

b. Applicant must not store payment card data anywhere on their network	Yes ☐	No ☐

FOR APPLICANTS WITH OVER $100,000,000 IN REVENUES, PLEASE COMPLETE THE FOLLOWING SECTION

22. Are vulnerability scans on all public-facing IP addresses carried out at least weekly?	Yes ☐	No ☐
23. Confirm that the applicant has an approved EDR solution deployed on all workstations and servers (see below for list of approved EDR solutions)	Yes ☐	No ☐

- Carbon Black
- CheckPoint Sandblast
- Cybereason EDR
- Cynet 360
- ESET Enterprise Inspector
- Fortinet FortiEDR
- McAfee MVISION
- Microsoft Defender
- Qualys Multi-Vector EDR
- RSA NetWitness
- Sentinel One
- Sophos Intercept X
- CrowdStrike Falcon
- FireEye Endpoint Security (HX)

24. Confirm the applicant has either Security information and Event Management (SIEM) or a Security Operations Center (SOC) in place		Yes ☐	No ☐
25. Confirm all generic passwords on local administrator accounts are removed (e.g. by deploying Microsoft LAPS)		Yes ☐	No ☐
26. If card-present transactions (i.e. in-store transactions) are accepted, applicant must confirm they have fully implemented an End-to-End (E2EE) or Point-to-Point (P2PE) encrypted Point-of-Sale (PoS) system	N/A ☐	Yes ☐	No ☐

E-CRIME QUESTION SET

27. If E-crime coverage is desired (only to applicants with no client monies), the following controls must be in place:		
a. Documented process that requires at least two members of staff to review and authorize any transactions above $10,000	Yes ☐	No ☐
b. Call-back provision in place for all transactions above $10,000 as well as any changes to payment details	Yes ☐	No ☐
c. Social engineering, phishing and business email compromise training provided to staff at least annually	Yes ☐	No ☐

IMPORTANT NOTICE AND SIGNATURE

The Applicant declares that the statements set forth herein are true. If any information in this Application changes prior to the inception date of any Policy issued by Underwriters, the Applicant will notify Underwriters of such changes and Underwriters may modify or withdraw any outstanding quotation. Signing of this Application does not bind the Applicant or Underwriters to complete any Policy, but it is agreed that this Application shall be the basis of the contract should a Policy be issued, and it will become part of any such Policy. All written statements and materials furnished to Underwriters in conjunction with this Application, or in conjunction with any prior application by the Applicant for insurance coverage, are hereby incorporated by reference into this Application and made a part hereof.

Authorized Signature of the Applicant (Must be a Principal or Officer of the Applicant)

Title of Signatory

Printed Name of Signatory

Date of Signature