Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

Cyber Security Application

Agent Name Agent Full Address

All questions MUST be completed in full. If space is insufficient to answer any question fully, attach a separate sheet.

Complete the applicant information below:

Full legal name of applicant:		Date:	
Inspection contact name:		Phone:	
Address:		City:	
State:		Zip code:	
Company website:		D&B No.:	
Email address:		NAICS:	

[ ] IT Director [ ] Director/Manager of Security Operations [ ] Director/Manager of IT Security

[ ] Security Analyst [ ] Information Security Director/Manager [ ] Other: _____

GENERAL INFORMATION

1. Describe in detail the applicant's business operations

2. a. Complete the following information for the applicant

	Most Recent Fiscal Year	Projection for Current Year	Next Year (Estimate)
Total revenue:	$	$	$
US revenue:	$	$	$
Foreign revenue:	$	$	$
Number of employees:			
Number of endpoints:			

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

b. Does the applicant handle the following types of data? [ ] Yes [ ] No

If yes, provide the number of records transmitted, received, and stored annually:

	Type Handled?	Number Transmitted	Number Received	Number Stored
Payment card information?	[ ] Yes [ ] No			
Financial or banking information?	[ ] Yes [ ] No			
Medical information (PHI)?	[ ] Yes [ ] No			
Biometric data?	[ ] Yes [ ] No			
Geolocation data?	[ ] Yes [ ] No			
Social Security/National Identification Numbers?	[ ] Yes [ ] No			
Other private data (PII)? (Describe)	[ ] Yes [ ] No			
Total				

3. Has the applicant within the past 12 months completed or agreed to, or does it contemplate entering into within the next 12 months:

   a. A merger, acquisition, consolidation, whether or not such transactions were or will be completed? [ ] Yes [ ] No

   If **yes,** provide a complete explanation detailing liabilities assumed and any liability coverage purchased by any predecessor organization:

   b. A change in the nature of business operations? [ ] Yes [ ] No

   If **yes,** provide details:

4. Does the applicant have written contracts for all service/product engagements with all customers?[ ] Yes [ ] No

   If no, what percentage of the time are written contracts used? _____%

DATA PRIVACY

1. Has the applicant designated a Chief Privacy Officer? [ ] Yes [ ] No

   If **no,** indicate what position is responsible for compliance with privacy regulations: _____

2. Does the applicant have a documented company-wide privacy policy? [ ] Yes [ ] No

   If yes, how often is the privacy policy reviewed? _____

3. Is the applicant compliant with all applicable international, federal, and state laws with regard to data transmission, storage, and disposal? [ ] Yes [ ] No

   If **no,** describe:

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

4. Which of the following are used to verify compliance with privacy regulations and notification?
   a. Internal counsel? [ ] Yes [ ] No
   b. Outside counsel? [ ] Yes [ ] No
   c. Automated privacy management software tool? [ ] Yes [ ] No

   If **yes,** which product(s) are used?:

5. Does the applicant have a process in place to allow customers to opt in/opt out of communications? [ ] Yes [ ] No

ACCESS CONTROLS

1. Has the applicant designated a Chief Information Security Officer (as respects computer systems and data security)? [ ] Yes [ ] No

   If **no,** indicate what position is responsible for computer and data security: _____
2. Does the applicant require multifactor authentication (MFA) for:
   a. Privileged user accounts? [ ] Yes [ ] No
   b. All Cloud recourses, including Office 365? [ ] Yes [ ] No
   c. All third-parties/vendors and contractors? [ ] Yes [ ] No
3. Does all remote access to the applicant's network and corporate email, including web applications, require MFA? [ ] Yes [ ] No
4. Does the applicant allow local administrative rights on workstations? [ ] Yes [ ] No
5. Has the applicant disabled remote desktop protocol (RDP)? [ ] Yes [ ] No

   If **no,** has the applicant implemented the following: [ ] VPN [ ] MFA [ ] RDP Honeypots
6. Do administrative/privileged accounts use a privilege access management (PAM) tool? [ ] Yes [ ] No

   If **yes,** which product(s) are used?
7. Is the applicant deploying a Zero Trust security framework requiring all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration before being granted or maintain access to application and data? [ ] Yes [ ] No
8. Is the applicant using the following features of a Zero Trust security framework, whether inside or outside the organization's network?
   a. Geo Fencing (by device, location, etc.)? [ ] Yes [ ] No
   b. MFA? [ ] Yes [ ] No
   c. Conditional access? [ ] Yes [ ] No
   d. Risk-based access controls? [ ] Yes [ ] No
   e. Access controls for SaaS application (i.e., CASB)? [ ] Yes [ ] No

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

INTERNAL SECURITY

1. Does the applicant use an Endpoint Detection and Response (EDR) tool? [ ] Yes [ ] No

   If **yes**:

   a. Which product(s) are used?

   b. Does the EDR have AI/Automated enforcement enabled? [ ] Yes [ ] No

      If **yes,** is it: [ ] Rules based [ ] Behavioral

   c. Indicate the percentage of the applicant's system that is visible to the EDR tool(s):

      Servers: _____% Endpoints: _____%

2. Does the applicant use an endpoint protection (EPP) tool? [ ] Yes [ ] No

   If **yes,** which product(s) are used?

3. Does the applicant use a data loss prevention (DLP) tool? [ ] Yes [ ] No

   If **yes,** which product(s) are used?

4. Does the applicant use Microsoft 365 in its organization?

   [ ] Yes. Have the following been implemented? [ ] MFA [ ] ATP [ ] Macros disabled by default

   [ ] No. Which products are used for email monitoring (e.g., Proofpoint)?

5. Does the applicant operate an SIEM monitored by:

   [ ] Dedicated SOC/MSSP (internal/external staff – on call rotations 24x7)

   [ ] Dedicated SOC/MSSP (internal/external staff – on call rotations 9x5)

   [ ] Internal IT staff receives email 24x7

   [ ] Internal IT staff receives emails, only responding when on the clock

   [ ] No monitoring

6. In what time frame does the applicant install critical and high severity patches?

   [ ] Within 2 weeks [ ] Within 1 month [ ] Within 2 months [ ] Other, describe: _____

7. If the applicant has any end of life or end of support software, is it segregated from the rest of the network? [ ] Yes [ ] No [ ] Partial [ ] N/A

8. What is the applicant's RTO for critical business systems?

   [ ] Less than 8 hours [ ] 8-12 hours [ ] 12-18 hours [ ] Greater than 18 hours

9. Does the applicant have a written:

   a. Business continuity plan? [ ] Yes [ ] No

      If **yes,** date last tested: _____

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

b. Disaster recovery plan? [ ] Yes [ ] No

If **yes,** date last tested: _____

c. Incident response plan? [ ] Yes [ ] No

If **yes,** date last tested: _____

d. Incident response plan for network intrusions and virus incidents? [ ] Yes [ ] No

If **yes,** date last tested: _____

Briefly describe the plans:

10. Are alternative facilities available for operations in the event of a shutdown or failure of the applicant's network? [ ] Yes [ ] No
11. Does the business continuity plan contemplate disruptions due to outsourced service providers? [ ] Yes [ ] No

    If **yes,** is it tested? [ ] Yes [ ] No
12. Does the business continuity plan require multiple/redundant outsourced service providers in place for the same services? [ ] Yes [ ] No
13. Does the applicant's incident response plan (IRP) specifically address ransomware scenarios? [ ] Yes [ ] No

    If **yes,** when was the date of last IRP with ransomware exercise: _____

    Outline any additional controls the applicant's organization has in place to mitigate the threat of ransomware attacks (e.g., tagging of external emails, DNS, network segmentation, vulnerability scanning, phishing training):
14. What is the largest number of records that the applicant holds in one segment? _____

    Is the applicant deploying: [ ] Segmentation [ ] Micro-Segmentation [ ] None of sensitive data
15. Does the applicant encrypt data:

    a. In transit? [ ] Yes [ ] No

    b. At rest? [ ] Yes [ ] No

    c. On mobile devices? [ ] Yes [ ] No

    If **no** to any of the above, provide details:
16. Does the applicant apply a least privilege access model to sensitive data? [ ] Yes [ ] No

    Provide details:

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

EMAIL SECURITY

1. Does the applicant authenticate emails using: [ ] SPF [ ] DKIM [ ] DMARC
2. Does the applicant have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end user? [ ] Yes [ ] No
3. Are external emails flagged? [ ] Yes [ ] No

BACKUP, RECOVERY, AND DATA PROTECTION

1. How frequently does the applicant back up critical data? [ ] Daily [ ] Weekly [ ] Monthly [ ] Other _____
2. Which of the following are used to store backups?

   [ ] Cloud storage [ ] Secondary data center [ ] Offline storage within a separate network segment
3. Does the applicant's backup strategy include the following?
   a. Segmentation? [ ] Yes [ ] No
   b. Encryption? [ ] Yes [ ] No
   c. MFA? [ ] Yes [ ] No
   d. Vaulted credentials? [ ] Yes [ ] No
   e. Tested for restore? [ ] Yes [ ] No
   f. Immutable? [ ] Yes [ ] No
   g. Scanned for malware? [ ] Yes [ ] No

   If **no** to any of the above, provide details including compensation controls:

SUPPLY CHAIN AND THIRD-PARTY/VENDOR MANAGEMENT

1. List the three largest technology vendors for critical business processes:
   a. _____
   b. _____
   c. _____
2. Does the applicant have a formal written third-party/vendor management policy in place that specifically addresses data security and ransomware? [ ] Yes [ ] No
3. Are contracts required of all third-parties/vendors? [ ] Yes [ ] No

   If **yes**:
   a. Does the applicant require third-parties with which it shares personally identifiable or confidential information to indemnify the applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party? [ ] Yes [ ] No
   b. What percentage of time are such contracted executed? [ ] 0-25% [ ] 26-50% [ ] 51-75% [ ] 76-100%
4. Does the applicant require that third-parties/vendors carry cyber security insurance? [ ] Yes [ ] No

5. Does the applicant conduct routine audits of third-parties/vendors? [ ] Yes [ ] No

   If **yes**:

   a. How often? [ ] Quarterly [ ] Annually [ ] Bi-annually [ ] Other _____

   b. Who performs the audit reviews? _____

6. Does least privilege apply to third-party/vendor access to the applicant's network? [ ] Yes [ ] No

7. Is dual authorization required for all wire transfers? [ ] Yes [ ] No

8. Are all changes requested by the vendor (including bank account, invoice changes, telephone or fax numbers, address, and other contact information) verified by the applicant by a direct call to the vendor using only the telephone number provided by the vendor before the request is received? [ ] Yes [ ] No

9. a. Identify the current provider for each of the following:

Anti-virus software:	Internet communication services:
Broadband ASP services:	Intrusion (EDR) detection software:
Cloud services:	Managed security services:
Collocation services:	Outsourcing services:
Payment card processing:	Website hosting:
Firewall technology:	Other (describe):

   b. Complete the following for Cloud services used by the applicant for payment card processing or storing private data:

Cloud Provider	Type	Service	No. of Records	Encrypted Storage
				[ ] Yes [ ] No
				[ ] Yes [ ] No

EMPLOYEE TRAINING

1. How often are phishing campaigns conducted?

   [ ] Never [ ] Monthly [ ] Quarterly [ ] Annually [ ] Ad Hoc

2. How often is security awareness training conducted for all staff?

   [ ] Never [ ] Monthly [ ] Quarterly [ ] Annually [ ] Ad Hoc

   Is fraudulent impersonation training included in security awareness training? [ ] Yes [ ] No

3. How often is phishing specific cybersecurity training conducted for elevated access users?

   [ ] Never [ ] Monthly [ ] Quarterly [ ] Annually [ ] Ad Hoc

PAYMENT CARDS – PCI/DSS

1. Is the applicant PCI compliant? [ ] Yes [ ] No

   If **yes,** what level and when was compliance achieved? Level: _____ Date: _____

2. Is segmentation used to isolate PCI information from the rest of the corporate network? [ ] Yes [ ] No

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

3. Does the applicant use a third-party vendor for e-commerce payment processing? [ ] Yes [ ] No

   If **yes,** provide the name of the vendor: _____

4. Is payment card data stored on the applicant's network? [ ] Yes [ ] No

   If **yes**:

   a. Is it encrypted at rest and in transit? [ ] Yes [ ] No

   b. Does the applicant apply a privileged access management security (PAM) tool for access? [ ] Yes [ ] No

5. Is payment card data encrypted at the point of sale (i.e., payment card reader or e-commerce payment portal) through transmission to the payment processor? [ ] Yes [ ] No

6. Is tokenization used to remove the actual credit card number from the transaction? [ ] Yes [ ] No

   If **yes,** provide the name of the vendor: _____

7. Has the applicant installed, maintained, and regularly updated firewall configuration and antivirus software to protect cardholder data? [ ] Yes [ ] No

MEDIA

1. Does the applicant use a third-party marketing or advertising agency? [ ] Yes [ ] No
2. Does the applicant provide any services to third parties related to media operations for a fee, (i.e., advertising or printing services, etc.)? [ ] Yes [ ] No
3. Are staff members with responsibility for content trained with respect to defamation, invasion of privacy, intellectual property, and other exposures? [ ] Yes [ ] No
4. Is any user-generated content uploaded to the applicant's websites? [ ] Yes [ ] No

   If **yes,** does the applicant review content? [ ] Yes [ ] No

5. Is the name, likeness, or portrayal of any real person, private location, audio recording, or trademark used in any content? [ ] Yes [ ] No

   If **yes,** are all intellectual property clearances obtained? [ ] Yes [ ] No

TECHNOLOGY

1. Provide the percentage of the applicant's revenues from each of the following categories:

Technology consulting and support General IT or security consulting, strategic planning, staffing or staff augmentation, training, help desk services, network support, configuration or installation	%	**Hardware** Design, manufacture, sell or repair devices or equipment, hardware recycling	%
Profess control PLC programming, system integration, manufacturing process control If any, also provide % of sales equipment	%	**Outsourced services** Data center, co-location, other managed services If any, also provide: % Platform as a Service (PaaS) % Infrastructure as a Service (IaaS/HaaS)	%
Custom software development Custom applications on behalf of clients or custom configuration of software If any, also provide: % hosted (SaaS/ASP) % deployed by client	%	**Packaged software development** Pre-packaged commercial or consumer applications If any, also provide: % hosted (SaaS/ASP) % deployed by client	%
Internet/web services Website design, creation, or hosting, search engine or SEO services	%	**Communications** ISP, VoIP, phone, wireless, cable, satellite services	%

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

2. Describe in detail the applicant's services, including primary purpose of any deployed software:

3. Indicate the applicant's four largest customer engagements for the past two years:

Client	Product/Service	Revenues
		$
		$
		$
		$

4. Do all of the applicant's clients provide written acceptance of all software or system development prior to production or implementation? [ ] Yes [ ] No

5. Indicate the percentage of the applicant's business using each type of contract below:

Applicant's standard contract/license agreement/letter of engagement:	%
Modified applicant letter of engagement:	%
Client contract agreement/letter of engagement:	%
Purchase order:	%
No contract:	%

6. Which of the following clauses are included in the applicant's standard contract wording?

[ ] Specified scope of services [ ] Payment terms [ ] Customer acceptance/final sign-off

[ ] Disclaimer of warranties [ ] Limitation of liability [ ] Project milestones

7. Does the applicant have a:

a. Policy for testing and documenting all software and system development? [ ] Yes [ ] No

b. Pre-implementation review or evaluation process in place? [ ] Yes [ ] No

c. Procedure for testing for security vulnerabilities throughout the lifecycle of the applicant's Products? [ ] Yes [ ] No

d. Formal process for customer complaint resolution? [ ] Yes [ ] No

8. Does the applicant perform background checks on all employees and contractors with access to sensitive data on the applicant's network or on client networks? [ ] Yes [ ] No

9. Has the applicant discontinued any product or software in the past five years? [ ] Yes [ ] No

If **yes,** explain:

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

OTHER INSURANCE

1. List current and prior cyber liability or cyber security insurance for each of the last 3 years:

   If **none,** check here [ ]

Insurance Company	Limit of Insurance	Deductible/SIR	Premium	Inception and Expiration Date	Retroactive or Prior Acts Date
	$	$	$		
	$	$	$		
	$	$	$		

2. Provide the following information:

Line of Business	Insurer	Limit of Insurance	Deductible/SIR	Inception and Expiration Date
General Liability	$	$	$	
Professional Liability	$	$	$	

3. Is the applicant aware of any loss, claim, suit, incident or notice of incident, arbitration proceeding, administrative proceeding, regulatory proceeding, or investigation against the applicant, its predecessors in business, any of the present or past partners, officers, employees, or any other individual who would fall under coverage proposed, or has any claim, suit, incident or notice of incident been made against the applicant or any staff member? [ ] Yes [ ] No

   If yes, provide full details:

4. Is the applicant aware of any facts, circumstances, incidents, situations, or data compromise which may result in any loss, claim, suit, or incident against the applicant, its predecessors in business, any of the present or past partners, officers, employees, or any individual who would fall under coverage proposed? [ ] Yes [ ] No

   If yes, provide full details:

5. Provide any additional information the applicant believes could be important for the Company to consider prior to making a coverage determination.

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

FAIR CREDIT REPORT ACT NOTICE

Personal information about you, including information from a credit or other investigative report, may be collected from persons other than you in connection with this application for insurance and subsequent amendments and renewals. Such information as well as other personal and privileged information collected by us or our agents may in certain circumstances be disclosed to third parties without your authorization. Credit scoring information may be used to help determine either your eligibility for insurance or the premium you will be charged. We may use a third party in connection with the development of your score. You have the right to review your personal information in our files and can request correction of any inaccuracies. A more detailed description of your rights and our practices regarding such information is available upon request. Contact your agent or broker for instructions on how to submit a request to us.

FRAUD WARNINGS

Applicable in AL, AR, DC, LA, MD, NM, RI and WV: Any person who knowingly (or willfully)* presents a false or fraudulent claim for payment of a loss or benefit or 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. *Applies in MD only.

Applicable in CA: For your protection, California law requires the following to appear on your application for insurance. 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.

Applicable in CO: 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.

Applicable in FL and OK: 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)*. *Applies in FL only.

Applicable in KS: 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 commits a fraudulent insurance act.

Applicable in KY, NY, OH and PA: 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 (not to exceed five thousand dollars and the stated value of the claim for each such violation)*. *Applies in NY only.

Applicable in ME, TN, VA and WA: 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 and denial of insurance benefits. *Applies in ME only.

Applicable in MN: A person who files a claim with intent to defraud or helps commit a fraud against an insurer is guilty of a crime.

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

Applicable in OR: Any person who knowingly and with intent to defraud or solicit another to defraud the insurer by submitting an application containing a false statement as to any material fact may be violating state law.

Applicable in VT: 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.

Normandy Insurance Services
4800 N Federal Hwy, Suite 302A
Boca Raton, FL 33431

Applicable in all other states: 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.

Representation Statement

The undersigned authorized officer of the applicant declares that the statements set forth herein are true to the best of his or her knowledge. The undersigned authorized officer agrees that if the information supplied on the application changes between the date of the application and the effective date of the insurance, he/she (undersigned) will immediately notify the insurer of such changes, and the insurer may withdraw or modify any outstanding quotations and/or authorization or agreement to bind the insurance. Signing of this application does not bind the applicant to the insurer to complete the insurance.

WARRANTY

The undersigned warrants to the Company that he/she understands and accepts the notice stated above and that the information contained herein is true and will be the basis of the policy and deemed incorporated therein, should the Company evidence its acceptance of this application by issuance of a policy. The undersigned authorize the release of claim information from any prior insurer to the Company or affiliates thereof.

This application is signed by undersigned authorized agent of the applicant(s) on behalf of the applicant(s) and its owners, partners, directors, officers, and employees.

This application must be signed by the owner, principal, partner, executive officer, or equivalent within 60 days of the proposed effective date.

_____ _____

Name of applicant Title

_____ _____

Signature of applicant Date

(Florida only) Agent license number: _____