CROMAR INSURANCE BROKERS SA

CYBER SECURE SOLUTION

www.cromar.gr

Coverholder at LLOYD'S

APPLICATION FOR CROMAR CYBER SECURE SOLUTION.

NOTICE: THE POLICY FOR WHICH THIS APPLICATION IS MADE IS A CLAIMS MADE AND REPORTED POLICY SUBJECT TO ITS TERMS. THIS POLICY APPLIES ONLY TO ANY CLAIM FIRST MADE AGAINST THE INSUREDS AND REPORTED IN WRITING TO THE UNDERWRITERS DURING THE POLICY PERIOD OR OPTIONAL EXTENSION PERIOD, IF APPLICABLE. AMOUNTS INCURRED AS CLAIMS EXPENSES SHALL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO THE DEDUCTIBLE. PLEASE READ THIS POLICY CAREFULLY.

Please fully answer all questions and submit all requested information.

I. GENERAL INFORMATION

1. APPLICANT:

Name:			
Address:		Country of Incorporation:	
Telephone:		Website URL's:	
Fax:			
Business Description:			

2. The following officer of the Applicant is designated to receive any and all notices from the Underwriters or their authorised representative(s) concerning this insurance:
3. The Applicant has continuously been in business since: _____/
(Month) (Year)
4. Please describe the Applicant's operations:
5. Applicant's Gross Revenues:

   For the calendar year or fiscal year ending day:_____ /mo:_____: €

   Previous year: _____Next year (est.):

   Estimated US/Canada revenues for latest year €

   Current number of employees:

   If the applicant is not publicly traded, please attach recent financial statements.

6. Are significant changes in the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes in the past twelve (12) months? Yes No
   If yes, please explain:

7. Has the Applicant in the past twelve (12) months completed or agreed to, or does it contemplate within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed? Yes No

   If yes, provide details:

II. MANAGEMENT OF PRIVACY EXPOSURES

1. Does the Applicant have a written corporate-wide privacy policy? Yes No

2. Does the Applicant accept credit cards for goods sold or services rendered? Yes No
   If yes:
   A. Please state the Applicant's approximate percentage of revenues from credit card transactions in the most recent twelve (12) months: _____%.

   B. If the Applicant accepts credit cards for payment of goods and services, is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards)? Yes No

      If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion:

3. Does the Applicant employ a chief privacy officer? Yes No

   If no, what position is responsible for management of, and compliance with the Applicant's privacy policies?

4. Within the past two years, has the Applicant undertaken any internal or external privacy or received any privacy certification? Yes No
   If yes, please describe:

5. Does the Applicant restrict employee access to personally identifiable on a business-need to know basis? Yes No

6. Does the Applicant require third parties with which it shares personally identifiable information 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

7. Is the Applicant aware of any release, loss or disclosure of personally identifiable information in its care, custody or control, or anyone holding such information on behalf of the Applicant in the most recent three year time period from the date of this Application? Yes No

   If yes, describe any such release, loss or disclosure:

III. Computer Systems Controls

1. Does the Applicant publish and distribute written computer and information systems policies and procedures to its employees? Yes No
2. Does the Applicant require positive acknowledgement from each employee of their understanding and agreement with the above policies and procedures? Yes No
3. Does the Applicant conduct training for every employee user of the information systems in security issues and procedures for its computer systems? Yes No

   If yes, indicate the frequency of such training :
4. Does the Applicant have :
   a. a disaster recovery plan? Yes No
   b. a business continuity plan? Yes No
   c. an incident response plan for network intrusions and virus incidents? Yes No
   How often are such plans tested?
5. Do the Applicant have a program in place to periodically test or audit security controls?

   Yes No

   If yes, please summarise the scope of such audits and/or tests:
6. Does the Applicant terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company? Yes No
7. Does the Applicant use commercially available firewall protection systems to prevent unauthorised access to internal networks and computer systems? Yes No
8. Does the Applicant use intrusion detection software to detect unauthorised access to internal networks and computer systems? Yes No
9. Does the Applicant utilise Anti-Virus software? Yes No

   If yes, is how often are virus signatures updated? Automatic Updates Weekly Monthly Other
10. Does the Applicant outsource any of its computer or network system operations or security?

    Yes No

    If yes:
    a. Please identify the operations outsourced and vendors:
    b. Does the Applicant require such vendors to demonstrate adequate security policies and procedures?

    Yes No
11. Is all valuable/sensitive data backed-up by the Applicant on a daily basis?

    Yes No

    If no, please describe exceptions:

12. Is at least one complete back-up file generation stored and secured off-site separate from the Applicant's main operations in a restricted area? Yes No

    If no, describe the procedure used by the Applicant, if any, to store or secure copies of valuable/sensitive data off-site?

13. Does the Applicant have and enforce policies concerning when internal and external communication should be encrypted? Yes No

    Are all laptop computers and portable media (e.g. "thumb drives") protected by encryption? Yes No

    Does the Applicant encrypt data "at rest" within computer databases? Yes No

14. Does the Applicant enforce a software update process including installation of software "patches"? Yes No

    If Yes, are critical patches installed within 30 days of release? Yes No

15. Has the Applicant suffered any known intrusions (i.e., unauthorised access or security breach) or denial of service attacks relating to its computer systems in the most recent three year time period from the date of this Application? Yes No

    If Yes, describe any such intrusions or attacks, including any damage caused by any such intrusions, including lost time, lost business income, or costs to repair any damage to systems or to reconstruct data or software, describe the damage that occurred, and state value of any lost time, income and the costs of any repair or reconstruction:…….....

IV. CONTENT EXPOSURES

1. Does the Applicant have a procedure for responding to allegations that content created, displayed or published by the Applicant is libelous, infringing, or in violation of a third party's privacy rights? Yes No

2. Does the Applicant have a qualified attorney review all content prior to posting on the Insured's Internet Site? Yes No

   If yes, does the review include screening the content for the following:

Copyright Infringement?	Yes	No
Trademark Infringement?	Yes	No
Invasion of Privacy?	Yes	No
Disparagement Issues?	Yes	No

   If no, please describe procedures to avoid the posting of improper or infringing content:

3. Within the last 3 years, has the Applicant ever received a complaint or cease and desist demand alleging trademark, copyright, invasion of privacy, or defamation with regard to any content published, displayed or distributed by or on behalf of the Applicant? Yes No

   If yes, please provide details regarding any such demands:

V. PRIOR CLAIMS AND CIRCUMSTANCES

1. Has the Applicant ever received any claims or complaints with respect to allegations of invasion of or injury to privacy, identity theft, theft of information, breach of information security, software copyright infringement or content infringement or been required to provide notification to individuals due to an actual or suspected disclosure of personal information? Yes No

   If yes, provide details of each such claim, allegation or incident, including costs, losses or damages incurred or paid, and any amounts paid as a loss under any insurance policy:

2. Has the Applicant been subject to any government action or investigation regarding alleged violation of any privacy law or regulation? Yes No

   If yes, please provide details of any such action or investigation:

3. Has the applicant ever experienced an extortion attempt or demand with respect to its computer systems? Yes No

   If yes, please provide details:

4. Has the Applicant notified consumers of a data breach incident in accordance with a data breach notification law in the past three (3) years? Yes No

5. No Applicant, director, officer, employee or other proposed insured has knowledge or information of any fact, circumstance, situation, event or transaction which may give rise to a claim under the proposed insurance except as follows:

   If no such knowledge or information, check here: None

CROMAR INSURANCE BROKERS SA

CYBER SECURE SOLUTION

www.cromar.gr

Coverholder at LLOYD'S

RANSOMWARE SUPPLEMENTAL APPLICATION

E-MAIL SECURITY

1. Do you pre-screen e-mails for potentially malicious attachments and links? ☐ Yes ☐ No
2. Do you provide a quarantine service to your users? ☐ Yes ☐ No
3. Do you 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
4. Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails? ☐ Yes ☐ No
5. How often is phishing training conducted to all staff (e.g. monthly, quarterly, annually)? _____
6. Can your users access e-mail through a web app on a non-corporate device? ☐ Yes ☐ No

   If Yes: do you enforce Multi-Factor Authentication (MFA)? ☐ Yes ☐ No
7. Do you use Office 365 in your organisation? ☐ Yes ☐ No

   If Yes: Do you use the o365 Advanced Threat Protection add-on? ☐ Yes ☐ No

INTERNAL SECURITY

8. Do you use an endpoint protection (EPP) product across your enterprise? _____
9. Do you use an endpoint detection and response (EDR) product across your enterprise? _____
10. Do you use MFA to protect privileged user accounts? ☐ Yes ☐ No
11. Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices? _____
12. What % of the enterprise is covered by your scheduled vulnerability scans? _____
13. In what time frame do you install critical and high severity patches across your enterprise? _____
14. If you have any end of life or end of support software, is it segregated from the rest of the network? _____
15. Have you configured host-based and network firewalls to disallow inbound connections by default? _____
16. Do you use a protective DNS service (e.g. Quad9, OpenDNS or the public sector PDNS)? ☐ Yes ☐ No
17. Do you use an endpoint application isolation and containment technology? _____
18. Do your users have local admin rights on their laptop / desktop? ☐ Yes ☐ No

19. Can users run MS Office Macro enabled documents on their system by default? _____

20. Do you provide your users with a password manager software? Yes No

21. Do you manage privileged accounts using tooling? E.g. CyberArk _____

22. Do you have a security operations center established, either in-house or outsourced? _____

BACK-UP AND RECOVERY POLICIES

23. Are your backups encrypted? _____

24. Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose? _____

25. Do you use a Cloud syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups? ☐ Yes ☐ No

26. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months? _____

27. Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware? _____

OTHER RANSOMWARE PREVENTATIVE MEASURES

Please describe any additional steps your organization takes to detect and prevent ransomware attacks (e.g. segmentation of your network, additional software tools, external security services, etc.).

ADDITIONAL INSURANCE COVERS

1. FRAUDULENT INSTRUCTION COVERAGE

Fraudulent Transfer.
Yes No

Please confirm that you already have the following in place, or will have the following in place prior to inception of cover:

Authentication of Contact and Bank Account Details: When originally set up, the accuracy of contact and bank account details is validated either fact to face OR through independent data (such as previously known telephone numbers or government issued ID)
Yes No

PRIOR to processing any payment/transfer all sort codes, account names and bank account numbers are validated to be the same as your company's internal records.
Yes No

A different means of communication to the original payment request or fund transfer demand is used to confirm the identity of the client.
Yes No

2. TELECOMUNICATION FRAUD

Telecommunication Fraud.
Yes No

Please confirm that you already have the following in place, or will have the following in place prior to inception of cover:

You have agreed a credit limit with your telecommunications carrier which if exceeded your telecommunications services will be suspended.
Yes No

PRIOR INSURANCE

1. Does the Applicant currently have insurance in place covering media, privacy or network security exposures?
Yes No

If yes, please provide the following:

Insurer	Limits	Deductible	Policy Period	Premium	Retroactive Date

2. Has any professional liability, privacy, network security or media insurance ever been declined or cancelled?
Yes No

If yes, please explain:

IMPORTANT NOTICE:

- It is your duty to disclose all material facts to Underwriters. A material fact is one which may influence an Underwriter's judgement in the consideration of your proposal. If your proposal is a renewal, it is likely that any change in facts previously advised to Underwriters will be material and such changes should be highlighted. If you are in any doubt as to whether a fact is material you should consult your broker or disclose it.
- Failure to so inform us may invalidate this insurance or any claim made under it.
- The particulars provided by, and statements made by, or on behalf of the Applicant(s) contained in this application form and any other information submitted or made available by, or on behalf of the Applicant(s) are the basis for the proposed policy and will be considered as being incorporated into and constituting a part of the proposed policy.

Privacy Policy of CROMAR Insurance Brokers SA.

CROMAR Insurance Brokers SA. (henceforth referred to as "the Company"), is committed to protecting the confidentiality of its customers. This current privacy policy details how we process Personal Data we collect, as part of our business activities.

What is Personal Data and how is it collected?

"Personal Data" is information that identifies you and relates to you or other persons (such as persons dependent on you). This Privacy Policy describes how we manage this personal data that we collect from various sources such as:

- insurance requests, claims requests, insurance policies, contracts of any type,
- telephone calls, e-mail messages and other means of communication, online or postal submission of CVs,
- service providers, insurance brokers, insurance advisors and agents, surveyors, technical advisors, health professionals, employers and other third parties,
- Public (Civil) and judicial services,
- from databases such as from the Statistical Service of Insurance Companies and the Auxiliary Fund Information Center,
- our website (www.cromar.gr),
- software applications which are available for your use,
- our social media and network pages
- and through other sources allowed by the current legislation and especially through the General Data Protection Regulation (EU) 2016/679.

Before you disclose to us the Personal Data of a third party, you must inform them of the contents of this Privacy Policy and obtain their consent respectively.

Who is the person responsible for processing Personal Data?

CROMAR Insurance Brokers SA, headquartered at 17 Ag. Konstantinou & Ag. Anargyron, 15124 Marousi, Greece, is responsible for processing your Personal Data.

Who is the Data Protection Officer?

If you have any questions regarding the handling of your Personal Data you can send an e-mail to dpo@cromar.gr or contact us by phone at 210 8028946 or by fax at 210 8029055.

How we use your Personal Data

We use your Personal Data to:

- communicate with you as part of our business
- send you important information relevant to how our insurance policies function
- evaluate insurance proposals and provide insurance services and support
- provide high quality service and training
- identify and prevent crimes related to fraud and money laundering, and to analyze and manage the insured risks
- carry out market research and analysis, including surveys regarding customer satisfaction
- facilitate the functionality of using social media
- manage complaints and requests for access to or correction of data
- comply with current legislation and regulations and respond to requests from public and government authorities
- protect our business operations and minimize our losses

Transmission of Personal Data

Your data will be passed on within our company to departments responsible for accepting the risk, for the proper and uninterrupted operation of your insurance policy and for your compensation such as: the underwriting, processing, claims, customer service department, etc.

Your personal data may be passed on to legal entities and / or persons with whom we maintain contracts for the proper servicing and compensation of our policyholders as well as for the assessment of a claim.

However, you should be aware that in this case, these legal entities and / or persons will process your personal data solely for the purpose of providing services to us and not for their own benefit, acting as data processors.

International Transfer of Personal Data

Due to our role and activity as Coverholder at Lloyd's, for the purposes outlined above, we may transfer Personal Data to third parties established in other European Union countries and the United Kingdom. In each transmission, we always take every step required to ensure that the data to be transmitted is always the minimum necessary and that the conditions for legitimate and lawful processing are always met.

Personal Data Security

CROMAR Insurance Brokers SA. will take appropriate technical, physical, legal and organizational measures that comply with the applicable privacy and security laws. Unfortunately, it is not possible to guarantee that it is 100% secure to transfer data over the Internet or other data storage system. If you feel that your personal information held by us has been compromised in any way, please notify our Company's Data Protection Officer. When CROMAR Insurance Brokers SA. provides personal data of its policyholders to a service provider for the management of the insurance policy, the provider will be carefully selected and will have to take appropriate measures to protect the confidentiality and security of this data.

What are your rights

You may at any time exercise the right to update, access and correct your Personal Data. In addition, and provided that the legal requirements are met, you can exercise:

- the right to delete your Personal Data
- the right to limit the processing of your Personal Data
- the right to Data Portability
- the right to object to processing, including automated decision making and profile development
- the right to withdraw your consent to processing at any time, without prejudice to the legitimacy of the consent-based processing before it is revoked
- the right to file a complaint with the competent Supervisory Authority

How long do we keep your Personal Data?

We ensure that the Personal Data we collect is processed for no longer than is necessary to meet the specific

purpose it was provided for and / or as required to comply with any record keeping obligation provided for by any applicable law.

Use of Cromar Electronic Services by Minors

Our e-Services are not intended for persons under eighteen (18) years of age, and we ask those persons not to provide Personal Information through our Electronic Services.

Use of Cookies

In order to personalize your visit to our website and to ensure the operation of certain features of our Website, we use "cookies" to collect and store data. For more information, please refer to our cookie policy, which is accessible on the official website of CROMAR Insurance Brokers SA (www.cromar.gr).

Changes to this Privacy Policy

We review this Policy regularly and reserve our right to make amendments at any time to take account of changes in our business activity and legal requirements. We will post the updates on our Website.

Declaration of Consent for the Processing of Personal Data

(The signing of this statement is necessary for the processing and operation of the policy)

As a Policy Holder / Insured I declare that:

1. I have read the "Information on the Processing of Personal Data" section of the insurance application.
2. I have been notified of the Processing of Personal Data by Cromar Insurance Brokers Ltd., and of the rights I have and maintain as a data subject (i.e. access, correction, deletion, restriction, portability and objection). Also, for my right to revoke at any time in the future the consent I hereby grant to this declaration as well as my rights referred to in Articles 12-22 of the General Data Protection Regulation.
3. I give my explicit consent (Article 7 of Regulation 2016/679) to the above Company for the following:
    a. For the processing of the Personal Data included in this insurance application, as well as any further data that might come to the knowledge of the Company in the future and is related to the insurance policy I am applying for, as well as to its operation.
    b. To keep records of all the above data in electronic or other form.

I acknowledge that the processing of Personal Data is absolutely necessary for the operation of the insurance policy I am requesting and that any revocation in the future will give the Company the right to terminate the insurance policy issued on the basis of it with immediate effect.

Full name Signature

Declaration of Consent for the Processing of Personal Data for Commercial / Promotional / Research Purposes

As a Policy Holder / Insured I declare that:

1. I have read the "Information on the Processing of Personal Data" section of the insurance application.
2. I have been notified of the Processing of Personal Data by Cromar Insurance Brokers Ltd., and of the rights I have and maintain as a data subject (i.e. access, correction, deletion, restriction, portability and objection). Also, for my right to revoke at any time in the future the consent I hereby grant to this declaration as well as my rights referred to in Articles 12-22 of the General Data Protection Regulation.
3. I give my explicit consent (Article 7 of Regulation 2016/679) to the above Company for the processing of the Personal Data included in this insurance application for commercial, promotional and research purposes, as well as to keep records of all the above data.

Full name Signature

THE UNDERSIGNED IS AUTHORISED BY THE APPLICANT AND DECLARES THAT THE STATEMENTS SET FORTH HEREIN AND ALL WRITTEN STATEMENTS AND MATERIALS FURNISHED TO THE UNDERWRITERS IN CONJUNCTION WITH THIS APPLICATION ARE TRUE. SIGNING OF THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE UNDERWRITERS TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THE STATEMENTS CONTAINED IN THIS APPLICATION, ANY SUPPLEMENTAL APPLICATIONS, AND THE MATERIALS SUBMITTED HEREWITH ARE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED AND HAVE BEEN RELIED UPON BY THE UNDERWRITERS IN ISSUING ANY POLICY.

THIS APPLICATION AND MATERIALS SUBMITTED WITH IT SHALL BE RETAINED ON FILE WITH THE UNDERWRITERS AND SHALL BE DEEMED ATTACHED TO AND BECOME PART OF THE POLICY IF ISSUED. THE UNDERWRITERS ARE AUTHORISED TO MAKE ANY INVESTIGATION AND INQUIRY IN CONNECTION WITH THIS APPLICATION AS THEY DEEM NECESSARY.

THE APPLICANT AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, THE APPLICANT WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE UNDERWRITERS OF SUCH CHANGES, AND THE UNDERWRITERS MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORISATIONS OR AGREEMENTS TO BIND THE INSURANCE.

I HAVE READ THE FOREGOING APPLICATION FOR INSURANCE INCLUDING ATTACHMENT 'A' AND REPRESENT THAT THE RESPONSES PROVIDED ON BEHALF OF THE APPLICANT ARE TRUE AND CORRECT.

WARNING

ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT (S)HE IS FACILITATING A FRAUD AGAINST AN INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT MAY BE GUILTY OF INSURANCE FRAUD.

Signed:

_____

Must be signed by corporate officer with authority to sign on Applicant's behalf

Date: _____ Day _____ Month _____ Year