GENERAL CONDITIONS OF CONTRACT

These General Terms and Conditions of **Contract (the "General Conditions of Contract** ") govern the acquisition by Cyber Guardian customers of the cybersecurity solutions included in the Cyber Guardian service (the " **Solutions** ") offered through the https://cyberguardian.tech Website (hereinafter, "Solutions"). the " **Website** ").

Likewise, these General Conditions of Contract contain the terms of the license of use with respect to the solutions offered by Cyber Guardian. In addition, the terms of the license for solutions based on vendor programs are regulated (to the extent not expressly provided herein) by the terms of the general conditions of those suppliers, which are located on the following websites: https://www.netskope.com/subscription-terms , https://www.crowdstrike.com/terms-conditions/ and http://www.mimecast.com/Contracts .

The right to use the Solutions is conditioned on your acceptance of the terms of the General Conditions of Contract. By using the Solutions, you (the " **Customer** ") acknowledge that you have read the terms contained herein and agree to be bound by them. If you do not agree with the terms stated, do not contract the solutions or use them.

The marking of the corresponding box in the contracting process, as well as the fact of telematically following all the steps thereof, implies the express acceptance of these General Conditions of Contract by the Client, having the same validity as its face-to-face and handwritten signature. In this way, the Client acknowledges to be a person with sufficient capacity to acquire the obligations derived from his actions through the Website, which he has previously read and understands its content.

1 COMPANY DATA

Owner: Cyber Guardian Solutions, S.L., (**"Cyber Guardian"**).

Registered office : Avda. De Cantabria s/n, 28660, Boadilla del Monte, Madrid,
Edificio Amazonia.

VAT number: ESB13978960.

Public Registry: Commercial Registry of Madrid Volume 45399, Folio 168, Sheet 798541, Entry 1.

E-mail: contact@cyberguardian.tech

2 OBJECT OF THE CONTRACT AND SOLUTIONS

These General Conditions of Contract regulate the contracting of solutions by companies and self-employed workers, so any regulation of consumer protection will not be applicable to them.

Cyber Guardian is a cybersecurity solution whose goal is to provide customers with advanced cybersecurity for devices, mail and navigation, the ability to know and manage their risks online and raise awareness among their employees.

By contracting the Cyber Guardian solution, Cyber Guardian undertakes to grant the customer an annual license on a number of solutions (in addition to the installation services thereof) which, at a minimum, include the following functionalities:

- Continuous monitoring of the customer's cybersecurity level in an intuitive dashboard to understand and manage their risks online, with alerts and recommendations for improvement and guidance.

- Device protection:

  .1 An advanced antimalware that scans the device, its internal memory and external storage devices, to detect and remove viruses, *ransomware* and Trojans known or not.
  .2 *Antispyware* to avoid spyware *malware*.

- Secure Mail: Email analysis tools that detect and block threats to prevent them from reaching users' inbox and with the following features:
  .1 *Antispam,* with detection and spam filter.
  .2 *Antiphishing,* with detection of emails with links or *malware* that are suspected to serve to steal credentials.

- Safe browsing: Inspection of web traffic during navigation:

  .1 *Content control* to block malicious web pages or dangerous file downloads;

  .2 *Antiadware* to avoid annoying or malicious ads.

- Threat analysis and detection: Allows to know the behavior of known and new threats.

- Network monitoring: Tools that analyze network traffic and alert threats.

- Initial configuration and security updates: Initial configuration for proper use, with respective malware signature updates and other threat detection data plus regular security software updates.
- Special training requirements: In addition to the common training requirements, the training provided to the customer includes a tutoring for the configuration of the security software, as well as a cybersecurity awareness kit and a phishing simulations

tool to train employees and complement the solution with human firewall skills.

3 HIRING OF SOLUTIONS

In accordance with the provisions of article 23 of Law 34/2002, of 11 July, for information society services and electronic commerce, contracts concluded by electronic means shall produce all the effects provided for by law when consent and other requirements for their validity are met.

In any event, the electronic medium containing the contract concluded electronically shall be admissible as documentary evidence in the event of a dispute between the parties.

For these purposes, it will be understood that the monitoring of all phases of the purchase process and, where appropriate, the payment of the corresponding economic quantity, necessarily imply the provision of the consent required for the contracting.

Similarly, and in accordance with the provisions of article 27 of Law 34/2002, on services of the information society and electronic commerce, all information relating to it is made available to users, prior to the start of the contracting procedure, that will only apply in the event that the User decides to proceed to the contracting through the Website.

- **Prior information**

Access to the contracting process is completely free, without any additional associated cost, apart from those of the user having an Internet connection.

To access the contracting process, the Customer must previously register on the Website in accordance with the procedure and under the conditions established in the Conditions of Use. Registration will be free and the credentials of the registered user will be personal and non-transferable. At the time of registration, the user must accept the privacy policy of Cyber Guardian, which describes both the treatments that will be made of the personal data of registered users and users who contract the solutions. Therefore, the customer will not be asked to accept the privacy policy again at the time of contracting the solutions. In case of doubts about the content of the privacy policy, it is available at all times through the link enabled at the foot of all sections of the Website.

All products marketed are perfectly described in their corresponding product sheets made available to users, not including those issues that expressly had not been indicated in them.

The contracting of the solutions must be carried out by accepting these General Conditions of Contract and the particular conditions of Cyber Guardian that will be shown during the contracting process (the " **Particular Conditions** ").

The Special Conditions offered in each case will be determined by Cyber Guardian depending on the circumstances of each order (e.g., depending on the number of devices or servers of the Customer), and they will be informed to the client in the contracting process once the client has provided the necessary data for its calculation and before the contracting is formalized .

The General Conditions and the Particular Conditions are understood to be accepted by the

Client at the time when the Client finishes the contracting procedure by pressing the "Contract Now" button, it is understood that the follow-up of all phases of the electronic contracting procedure and the inclusion of all the requested data imply, together with the marking of the corresponding box relating to acceptance, a direct manifestation of the willingness of the client to accept them.

Upon completion of the contracting process, the Customer will receive via email a copy of the General Conditions of Contract and the Particular Conditions in durable support. You can also access the set of signed conditions and active subscriptions from your Cyber Guardian user profile.

Cyber Guardian will introduce adequate and sufficient technical means to identify and correct technical errors in the management of information as soon as it is responsible.

The language in which the contracting procedure will be processed and in which this contract is formalized will be, unless otherwise indicated, English.

- **Purchase procedure**

The procedure for contracting solutions is carried out electronically through the Website. Any person with Internet access and registered on the Website can carry out the hiring.

The complete procedure to be followed by all users who wish to acquire any of the solutions offered through the Website will be the following:

1 To be able to personalize the purchase and have all the user's data, the user must log in, if already registered on the Website, entering their username and password. If, on the other hand, you do not have a user account, you must register as such, providing a series of personal data considered essential to identify yourself as a contractor.

2 Once the User has accessed the Website and has logged in with his User and credentials, he must select the subscription plan that interests him and customize the options that are required, being very important to review its description, as well as its characteristics, conditions and final prices.

3 Then, the User must read and expressly accept these General Conditions of Contract by marking the corresponding box provided for this purpose.

4 Then, once the solution you wish to acquire has been chosen and the General Conditions of Contract accepted, the User must start the electronic purchase process, for which he must only click on the button "Contract Now", at which time they will be understood accepted, in addition, the Particular Conditions generated during the process.

5 The user must only make the payment following the instructions of the web. At no time will Cyber Guardian have access to your bank details, which are directly managed by the corresponding banking entities in our payment gateway.

6 Once the purchase is finished, a summary screen of the purchase made will be displayed, without prejudice to the fact that the user will automatically receive an email confirming that the purchase has been made successfully. In this email the purchase made will be described, as well as the characteristics of it, and this document will serve as accreditation for any type of claim. If you do not receive such email , please check your *spam or spam inbox* and, if it is not in this section, please let us know as soon as possible so that we can solve the problem.

7 The customer will be able to find all the information of his purchase, as well as of his active subscriptions, in his Cyber Guardian user profile, where, after identification, he will be able to see the summary of the purchase, the start date and the end of the subscription period, the annual cost of the subscription and the status of the subscription.

8 Once the purchase is completed, the license will be activated within a maximum period of 24 hours , unless, within that same period, the authorizations required by the corresponding suppliers have not been received. In the latter case, the license will be activated as soon as the above authorizations are received.

4 FREE TRIAL

The contracting of the demo and free version of the solutions, available to those customers who access the Website with the corresponding promotional code, it will not imply any cost to the Client and will be subject to the limitations that are informed in the contracting process of the same and of the Particular Conditions that in each case are specified.

Without prejudice to the applicability of these General Conditions of Contract, in the event of a conflict about free demo versions between the information provided on the Website or in the Particular Conditions with these General Conditions of Contract, the information provided on the Website and in the Particular Conditions will prevail.

To proceed with the purchase of the demo version, the client must register to access the solutions, providing the personal data that are requested in the registration form and that will be treated in accordance with the provisions of the privacy policy that must be accepted, together with these General Conditions of Contract, to register. The registration process is free and will take place in English. Once the acceptance box of the aforementioned legal texts has been checked, the contract can be completed by clicking on the "Create Account" button, through which the Particular Conditions shown during the activation process of the free trial will also be accepted.

In case you want to opt for the full version of the solution, the purchase process must be carried out in accordance with what is indicated in the previous section.

5 BANCO SANTANDER CUSTOMERS

Banco Santander will transfer to Cyber Guardian the data of the clients that are requested in forms enabled in the platform for the contracting of the solutions, in order for Cyber Guardian to formalize the contracting and proceed to the provision of the services in accordance with the conditions established in this contract.

In addition, we expressly inform you that Cyber Guardian will transfer the customer data, provided that the client is a legal person or that the data has been previously anonymized, in order to manage and coordinate the business relationship between Cyber Guardian and Banco Santander.

6 PRICE AND BILLING OF SOLUTIONS

The annual price of the license on the offered solutions is reported on the Website during the contracting process, once the customer provides a series of data about the order you want to place, to the extent that the price reported will depend on the circumstances and needs of each customer.

In this sense, Cyber Guardian will break down the different concepts and their amounts, as well as the applicable taxes and, where appropriate, subsidies, thus informing the Customer of the total cost of the Service (" **Annual Total Cost** ").

All prices shown are final product prices, being expressly excluded the Value Added Tax (VAT) and the General Indirect Canary Tax (IGIC), which will be reported in a disaggregated manner. Notwithstanding the foregoing, the final price of an order will include all those increases or discounts that are applicable, expenses passed on to the customer and additional expenses for accessory services, means of payment, etc. In any case, all these amounts will be shown to the client in a broken down manner during the contracting process.

The contract will be perfected by payment of the total annual cost.

7 INTELLECTUAL AND INDUSTRIAL PROPERTY

Cyber Guardian owns or, where appropriate, holds the corresponding licenses on the rights of exploitation of intellectual and industrial property of the Solutions, as well as the rights of intellectual and industrial property on the information, materials and contents thereof, including, among others, trademarks, trademarks and other products. trade names and other distinctive signs, images, photographs and videos and texts written in any language, including programming codes.

In no case shall it be understood that the reproduction, distribution, public communication or transformation of the above mentioned materials to the Client or by part of the latter implies a waiver, transmission, license or total or partial transfer of said rights by Cyber Guardian and, in particular, is prohibited (except as permitted by applicable law) modify, copy, reproduce, publicly communicate, transform or distribute, by any means and in any form, all or part of the contents included in the Solutions, for public or commercial purposes if you do not have the prior, express and written authorization of Cyber Guardian , your case, the owner of the corresponding rights.

However, the Customer is granted a right to use the content and/or services of the Solutions, as well as the Solutions themselves under the terms of paragraph 8 below, within an area strictly necessary for the execution of the obligations and rights assumed by the parties when subscribing both the General Conditions of Contract and, where appropriate, the Particular Conditions.

In the event that the Customer uses any intellectual or industrial property right at the time of exercising its obligations or contractual rights with Cyber Guardian, the Customer declares, guarantees and agrees that he has the right to do so freely, that such information does not infringe any intellectual property rights, industrial, trade secret or any other rights of third parties, and that such information is not confidential or harmful to third parties.

The Client acknowledges to assume responsibility, leaving Cyber Guardian and the Suppliers harmless, for any exploitation of intellectual or industrial property rights that it carries out, reaching such responsibility without any restriction the accuracy, legality, originality and ownership thereof.

8 LICENSE TO USE THE SOLUTIONS

- **Definitions**

For the purposes of this clause, the following terms shall have the following meanings:

- Updates: Fixes, and other updates to the solutions, as well as any new versions of the solutions, as long as Cyber Guardian makes them available to its active license customers.

- Customer Data: Any data (including personal data), databases, documents, files, records, documentation or information of any nature owned or controlled by the Client, that the Client enters or collects through his use of the Solutions under the terms of these General Conditions of Contract.

- Documentation: Materials and text of help for the solutions made available to the client and / or authorized persons.

- Cyber Guardian: Cyber Guardian Solutions, S.L., Spanish entity with registered office at Avda de Cantabria s/n, 28660, Boadilla del Monte, Madrid, Edificio Amazonia and VAT number ESB13978960. Cyber Guardian is the owner and licensor of the solutions and documentation licensed to the client under these General Conditions of Contract.

- License Period: Period covered by the price paid by the Customer, during which he/she is entitled to use the purchased Solution.

- Authorized persons: Employees of the Customer to whom the Customer has expressly authorized and granted access to the Solutions for use.

- Term: Period during which the license is in full force and effect. The term is the sum of successive leave periods.

- Solution(s): Software package(s) owned by Cyber Guardian, (and software package(s) from suppliers over which Cyber Guardian has acquired a sufficient license or exploitation right), the functionalities of which are described in clause 2 of these General Terms and Conditions of Contract, that Customer is licensed under the terms of this clause and for the term, including updates to the Solutions that Cyber Guardian may make available to Customer from time to time.

- Support: Support provided by Cyber Guardian as described in Section 9 (“ **Support Services** ”).

- **Granting of the license**

The Parties acknowledge that Cyber Guardian owns the existing intellectual and industrial property rights over any creative, distinctive or inventive elements incorporated into the Solutions and Documentation, or that it has the third party licenses necessary to subscribe to these General Terms and Conditions of Contract and, in particular, this clause.

Subject to payment of the price for the purchased Solution, Cyber Guardian grants the Customer a non-exclusive, non-transferable right to use such Solution for the period of one (1) year and for the Client's commercial purposes (Solutions are exclusively aimed at companies and self-employed workers). and in relation to the functionalities and purposes of the solution. In any event, the Customer shall only have the right to use the Solution internally, in accordance with the terms of this License and any other terms that may be established in any applicable supplementary document or annexes thereto.

The above license grant expressly excludes any right to rent, sublicense, lease, assign, transfer, display or distribute or make the Solution available to third parties. The Customer (except as permitted by applicable law) will not alter, modify, manipulate or adapt the Solution, including without limitation its translation, decompilation, disassembly, elaboration of derivative works or reverse engineering of the Solution and its associated materials. The granting of the license also excludes making comparative assessments or analyzes (including benchmarking) or any other analysis intended for external use or publication. The above prohibitions extend to documentation that can be made available to the customer.

The Client acknowledges that the license granted under these General Conditions of Contract is not a perpetual license and consequently does not have the right to retain or use the Solution and, where appropriate, the documentation, including all materials and elements thereof, after the end of the term. The Customer shall not give access to the Solution to any User other than an Authorized Person who is using the Solution exclusively for the benefit of the Customer. In any event, the Customer agrees to notify Cyber Guardian as soon as it becomes aware of any unauthorized use of the License.

The Solution, or parts thereof, may have been developed by an independent third party who owns copyright and other similar proprietary rights thereto (the “ **Supplier** ”). In this regard, any infringement of such rights by the customer, including authorized persons, could be the subject of a complaint by the supplier. The Customer agrees that the Solution and any proprietary information contained therein are the sole and exclusive property of their respective owners or developers (among others, the Providers) and also constitute Confidential Information. The Client agrees that any Solution Technology Provider is a third party beneficiary of these General Terms and Conditions of Contract and that, as such, such Provider may enforce any provision of this clause.

This grant of license does not transfer to the Client any rights over the Solutions, except for the limited use license granted by means of these General Conditions of Contract. All rights not expressly granted to the Customer under these General Conditions of Contract are reserved

by Cyber Guardian or by the applicable Supplier.

- **Customer data**

Customer Data generated or collected as a result of Customer's use of the Solution will remain the exclusive ownership of Customer and all intellectual property rights thereto will and will continue to be vested in Customer.

Notwithstanding the foregoing, Customer expressly agrees that Cyber Guardian shall have the right to generate patterns, trends, knowledge, metadata and other ideas (i) by anonymizing, where appropriate, Customer Data; (ii) by aggregating anonymized Customer Data with other data; and/or (iii) based on learning, records and anonymous data about the use of Cyber Guardian products and/or services (" **Cyber Guardian Data** "). Cyber Guardian data will only consist of anonymous data that does not identify the customer, its consumers and/or authorized persons, or any other personally identifiable information. Anonymized data is data from which any information that may identify the customer or a natural person is deleted, and the remaining data is data from which an individual cannot be identified, either by the customer or by any other person (i.e. not all probable means of reidentification are possible). Cyber Guardian data will belong to Cyber Guardian, who may use such data for any commercial purpose during or after the term (including, but not limited to, developing, providing, operating, operating, maintain and improve Cyber Guardian products and services and create and distribute reports and other materials).

In this regard, to the extent necessary, the Customer grants Cyber Guardian a worldwide, royalty-free, perpetual and irrevocable license to the Customer Data to enable its use by Cyber Guardian for the purposes indicated above.

- **Restrictions of use**

It is expressly prohibited to use the Solutions for illegal or unauthorized purposes. In particular, but without limitation, the following actions are not allowed:

1 Use of the Solutions in any manner that may cause damage, interruptions, interference, inefficiencies or defective operation of the same or the device of a third party (among others, Cyber Guardian or the suppliers).

2 Use of the Solutions for the transmission, installation or publication of any virus, malicious code or any other harmful file or component.

3 Use of solutions to harm, threaten, harass, abuse, stalk, defame or infringe or violate the rights of any person or organization.

4 Unauthorized access or use of any section, component or element of the Solutions through any illegitimate means.

5 Modification of Solutions, Documentation or any of their elements, including prohibition of creating derivative works based on Solutions.

6 Use of the solutions in any way that contravenes the terms of these General Conditions of

Contract, the law, morality, generally accepted customs and social norms, or public order.

7 Use of the Solutions in any manner that may constitute an infringement of any intellectual property rights of Cyber Guardian or its provider(s).

8 Develop software or software applications , or any invention that integrates software applications or computer programs, with functionalities similar to those of the Solutions.

9 Register trademarks, trade names or any other distinctive signs associated with the Solutions.

The Client acknowledges that failure to comply with the restrictions described in these General Conditions of Contract will imply, at the discretion of Cyber Guardian, the termination of the contractual relationship and, consequently, the termination of the license granted under them, as set forth below.

In order to enable Cyber Guardian to effectively monitor and defend its intellectual property rights, the Customer expressly authorizes Cyber Guardian to collect information about the Customer's use of the Solutions , including the devices used to access the Solutions, the connection times and parameters, and any other data that Cyber Guardian may reasonably consider appropriate for these purposes.

9 SUPPORT SERVICES

Cyber Guardian offers the Customer a technical and commercial support service, through which it will pay due attention to the queries, complaints, problems and suggestions of the Customer in relation to the solutions according to the nature of the same. Access to Support Services will be available through the following means:

- Technical support: support@cyberguardian.tech
- Commercial support: contact@cyberguardian.tech

During the following working hours: Monday to Friday: 8:00 – 20:00 (GMT +1) excluding national holidays in Spain.

Cyber Guardian Support Services will respond to complaints or inquiries received in the shortest possible time and will endeavor to prevent such time from exceeding a period of 2 days from the time the claim or inquiry was filed.

The Customer undertakes not to perform any maintenance without the prior written consent of Cyber Guardian (except where permitted by applicable law). In this sense, any maintenance (not allowed) performed by the Customer, authorized person or external supplier of the Customer (other than the Suppliers) will constitute a material breach of these General Conditions of Contract and may involve the termination of the license granted in this document. The Customer acknowledges and agrees that Cyber Guardian shall not be liable, to the extent permitted by applicable law, for faults, defects, malfunctions of the Solutions, of any kind, that may arise from unauthorized maintenance tasks performed by the

Customer, nor any damage or loss arising from such failures, defects or malfunctions.

Cyber Guardian shall not be obliged to provide Support when faults, defects or malfunctions are caused by misuse , negligence or breach of the terms of these General Conditions of Contract by the Client and/or its authorized persons, including any use that contravenes the terms of these General Conditions of Contract, applicable law and / or instructions, guidelines or recommendations made by Cyber Guardian are or are not included in the documentation. In addition, Cyber Guardian shall not be obliged to provide Support under the terms provided herein in the event of force majeure events or other external factors affecting the availability or functionality of the Solutions.

10 CONFIDENTIAL INFORMATION

Cyber Guardian and the Client will undertake, both during the duration of the contractual relationship, and after the termination thereof, to treat under the strictest confidentiality all data, information and documents that the parties exchange with a view to the provision of contracted services.

Each Party (the " **Receiving Party** ") accepts and declares that it will keep confidential all information, in any format, documents, programs, products, products, equipment, tests, evaluations, prototypes , samples, formulas, specifications, processes, know-how, software and hardware, technical descriptions, data, trade secrets, past, present and future investigations, developments, information about the business and/or activities of the parties, commercial information, business plans , strategies, methods and/or practices, as well as, in general , any information that is not in the public domain, such as, but not limited to, employee data, product data, services, marketing strategies and/or future business plans and/or customers, including customer listings, accounts, costs, sales and any other customer or financial information related to the business of the parties obtained or disclosed to it by the other party (" **transmitting party** ") in the context of the provision of services (" **Confidential Information** ").

The receiving party of the confidential information undertakes not to use the confidential information for purposes other than those arising from the provision of services, and not to disclose, deliver or supply it, in whole or in part, to third parties (during the contractual relationship between the Parties and after its termination, indefinitely), unless the prior written authorization of the transmitting Party of such confidential information is obtained.

In case of termination of the contractual relationship for any reason, the receiving party undertakes to deliver within thirty (30 days) to the transmitting party and / or destroy, at its request, all confidential information that, as a result of them, it is in its possession or in the possession of its employees, without the receiving party having the right to retain any copy of the said confidential information.

In order to ensure confidentiality, the receiving party undertakes to:

a Ensure that only members of its staff and third parties authorized by the transmitting party will have access to confidential information.

b Inform both the members of its staff authorized for such access about the confidential nature of the information and their responsibilities.

c Not to disclose or exploit, whatever the modality, the confidential information provided by the transmitting party and the results or relationships derived from it .
d Do not make copies or duplicates of confidential information, unless it is essential for the provision of solutions.

The obligation of confidentiality provided herein is excluded from the information received by the receiving party that:

a It is known to it prior to its transmission, provided that the receiving party can justify possession of the information;
b information of general or public knowledge;
c it has been received from legitimate third parties who own it, without being obliged to confidentiality;
d It has been developed independently by the receiving Party without having used all or part of the information of the other Party;
e The transmission of which to third parties has been approved or consented in advance and in writing, generally and without restriction, by the transmitting party ;
f It is necessary to provide together with a judicial claim arising from a conflict between the parties, when confidential information is relevant to the resolution of such a conflict, and/or has been requested by an administrative or judicial authority. In the latter case, the party receiving such a request shall inform, whenever possible, the other party in advance and, in any event, as quickly as possible and provided that the nature of the administrative or judicial proceedings so permit.

11 PROTECTION OF PERSONAL DATA

Cyber Guardian and the Customer undertake to comply fully with the obligations established in Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation, GDPR), with Organic Law 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights (LOPDGDD) and in any other applicable legal obligation in the field of data protection, as well as those established in this clause and in any complementary condition.

Each of the parties will be responsible for the processing of the personal data collected from the other party in order to manage the contractual relationship established, keeping the data during the validity of these General Conditions of Contract and, where appropriate, the Particular Conditions and, once this is finished, for the subsequent time that is legally necessary for the possible attention of the responsibilities derived from the treatment carried out. The data may be communicated to public authorities on the occasion of compliance with the contractual relationship or by legal obligation .

Interested parties are informed of their rights to request access to their data, their rectification, cancelation, deletion or limitation of their treatment, or to oppose the treatment, as well as the right to data portability. Likewise, the interested parties shall have the right to file a free claim with the Spanish Data Protection Agency (www.aepd.es) when they consider that any of their rights have been violated or have been treated in some illegitimate way .

For the exercise of your rights, as well as to request any information regarding the processing

of your data, the interested parties may contact each of the controllers or their data protection officer, if they have it, through the contact points indicated in their respective privacy policies. Cyber Guardian's privacy policy can be found at politica-de-privacidad.pdf (cyberguardian.tech)

In addition, the provision of the solutions involves the processing by Cyber Guardian of personal data responsibility of the customer, including the registration, consultation, storage, and deletion of personal data, insofar as it is necessary for the execution of the same and until its completion , in respect of which Cyber Guardian will be considered in charge of the treatment. For this purpose and in compliance with the provisions of Article 28 of the GDPR, this data processing will be carried out in accordance with the stipulations included in the Processing Order Agreement placed as an Annex in these General Contracting Conditions.

12 ENTRY INTO FORCE AND CONTRACT TERM

These General Conditions of Contract will be applicable from the date of acceptance of them, at the end of the contracting process.

The contract shall remain in force for the period of one (1) year, which shall be automatically extended for successive periods of one year, unless either party expresses its intention not to extend it at least thirty (30) calendar days in advance, or it is resolved in advance in accordance with the grounds for resolution described in paragraph 13 below (' **early termination** ').

13 AMENDMENT

Without prejudice to the modifiability of the Particular Conditions, Cyber Guardian reserves the right to modify or terminate, at its sole discretion, the terms of the General Conditions of Contract, for which it will communicate the new conditions by publishing them on the Website in the same way in which these General Conditions of Contract appear.

14 EARLY RESOLUTION

In addition to the legally foreseen causes, these General Contracting Conditions may be resolved in the following cases:

i Resolution for convenience . The Customer may terminate these General Conditions of Contract at any time, subject to payment of any license or service price pending on the date of termination, providing prior written notice to Cyber Guardian at least [30] days prior to the expiration of the then-current license period.

ii Resolution for non-compliance . Cyber Guardian may terminate these General Conditions of Contract if the Client breaches any provision thereof and fails to remedy such breach within fifteen (15) days from the date of sending the corresponding written

notice. Such termination by Cyber Guardian will not exempt Customer from paying any outstanding license or service fees. Likewise, during the remediation period Cyber Guardian reserves the right to suspend or restrict the client's access to the contracted solution/s

iii Resolution by interruption of solutions . In the event that Cyber Guardian and/or the Supplier decide to discontinue the solution purchased by the Customer, Cyber Guardian may terminate these General Conditions of Contract.

Customer's right to use the Solutions will automatically terminate on the termination date, for any reason, and Cyber Guardian will be entitled to terminate Customer's access to the Solution in question, regardless of whether it is in the Customer 's possession or control or Cyber Guardian.

Upon termination, and at Cyber Guardian's option, Customer shall, if applicable, return or destroy all copies of the Software and Documentation to Cyber Guardian, or destroy it and provide Cyber Guardian with a certificate of destruction for all such copies of the Software and Documentation.

In addition, Cyber Guardian reserves the right to suspend access to the Solutions immediately, to protect the systems of Cyber Guardian or any of its provider(s), in the event that the systems of any client are subject to significant threats to security, integrity, functionality or availability of the Solutions or if the activities of the Customer violate any of the restrictions of use described in section 8.

15 RESPONSIBILITY OF THE PARTIES

Any breach of the applicable law, the General Conditions of Contract or the Particular Conditions by any of the parties, as well as any culpable or negligent act or omission, it will entitle the other party to demand from the non-performing, at-fault or negligent party compensation for any damages, losses, lost profits, contractual or tort liability to third parties, costs, expenses, expenses, and other costs. administrative sanctions or any other harm suffered as a direct or indirect consequence of such breach or culpable or negligent act or omission.

In particular, the Customer shall be responsible for:

a Any act that contravenes the content of the General Conditions of Contract or the Particular Conditions, the law, morality, generally accepted customs or social norms and public order.

b Any damage or loss that may arise from misuse, negligence or non-compliance by the Client in his use of the Solutions, including, but not limited to, the terms of the General Conditions of Contract, the Particular Conditions, as well as the general conditions of the Suppliers, applicable law and/or any instructions, guidelines or recommendations made by Cyber Guardian, whether or not included in the documentation.

c Accuracy and completeness of the information provided by the Client when accepting and executing the General Conditions of Contract and the Particular Conditions.

d Compliance with the terms of the General Conditions of Contract and Particular Conditions, including payment of the corresponding license fees.

The Client agrees to indemnify, defend and hold harmless Cyber Guardian, including its officers, directors, shareholders, successors, affiliates, employees, agents and representatives, of and against any costs, claims, demands, liabilities, expenses, losses, damages, including attorneys' fees, arising out of or resulting from the use of the Solutions by the Client. The Client also agrees to indemnify Cyber Guardian for the legal fees incurred by Cyber Guardian, acting reasonably, in the investigation or application of its rights under these General Conditions of Contract and Particular Conditions.

To THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL Cyber Guardian OR ITS TECHNOLOGY OR SOFTWARE SUPPLIERS BE LIABLE FOR ANY LOSS, COST OR DAMAGES, INCLUDING WITHOUT LIMITATION INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL business interruption, loss of data, computer failure, damage or malfunction, or any claim by any party, arising out of the use of, or inability to use, the Solutions , software or associated documentation, even if the Customer has warned of it. In no case shall the liability of Cyber Guardian or that of its suppliers exceed the amount of consideration actually paid by the client under the General Conditions of Contract and Particular Conditions. The warranty and remedies set forth herein are exclusive and supersede all others, oral or written, express or implied.

Without prejudice to the foregoing, the parties acknowledge that the object of these General Conditions of Contract, as well as of the Particular Conditions, is the installation of the solutions described in these General Conditions of Contract, according to market standards and state of the art, Cyber Guardian commits to use its best efforts to seek the greatest effectiveness of them.

However, in no case can Cyber Guardian be held responsible for security breaches that occur as a result of attacks by third parties or human errors by Cyber Guardian personnel or third parties in the application of security measures implemented in the solutions. In this sense, the parties acknowledge that the obligations assumed by Cyber Guardian regarding the provision of the solutions are obligations of provision of means, and not of result.

In this regard, the Parties acknowledge that Cyber Guardian Solutions are not designed or intended for use in hazardous environments requiring fail-safe performance or operation. Cyber Guardian products are not intended for aircraft navigation operations, nuclear facilities or communication systems, weapons systems, direct or indirect life support systems, air traffic control or any application or installation where a failure could result in death, serious physical injury or property damage.

Under no circumstances will the parties be liable for indirect, consequential, incidental, punitive and/or any other category of special damages, loss of profits, damages that may occur as a result of any breach of the General Conditions of Contract, of the Particular Conditions or of the Agreement due to force majeure.

The parties mutually guarantee that, at all times, they will be aware of the payment of their obligations to the Tax Agency and Social Security, exonerating the other party from any liability generated as a result of any judicial or extrajudicial claim of third parties for these concepts.

Finally, the Client guarantees that at the date of subscription of these General Conditions of Contract is not a competitor of Cyber Guardian or its provider(s) and acknowledges that Cyber Guardian can terminate this license in advance by changing this situation.

16 SAFEGUARD CLAUSE

In the event that one of the clauses or extremes of these General Conditions of Contract or of the Particular Conditions is declared null and void by judicial decision or final arbitral resolution, the rest of the stipulations will not be affected. In this case, the affected clause or clauses will be replaced by another or others that preserve the effects pursued by the Conditions of Contract of the Website.

17 APPLICABLE LAW AND JURISDICTION

These General Conditions of Contract and the Particular Conditions, as well as any relationship between the Client and Cyber Guardian, will be governed by Spanish law and any conflict arising from them will be submitted to the Courts and Tribunals of Madrid city.

ANNEX

DATA TREATMENT ORDER AGREEMENT

I The Parties acknowledge that by virtue of this Processing Order Agreement (" **Annex** "), Cyber Guardian (" **Processor** ") has granted to the Customer ("Processor") a license on the software owned by the Processor, and has undertaken to provide the Data Controller with the associated hosting services in connection with the use of the software by the Data Controller (hereinafter referred to as the " **Services** ").

II That, in the execution of these Services, the Processor needs to process certain personal data that are the responsibility of the Controller.

III That, in order to regulate such access, both Parties agree to incorporate this Annex to the General Contracting Conditions, which will be governed by Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, (hereinafter, the "GDPR"), its implementing regulations and, in particular, the following

CLAUSES

FIRST. DEFINITIONS

1.1 Applicable Data Protection Legislation : Means any law and regulation of privacy and data protection applicable to the Parties in relation to this Annex and, in particular, the GDPR, Organic Law 3/2018, of December 5, protection of Personal Data and Guarantee of Digital Rights, and any other applicable national law or regulation.

1.2 Personal data of the controller: Personal data provided by the controller to the processor for the purpose of carrying out the services under the agreement.

1.3 Special categories of data: Personal data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, and/or data relating to the health or sexual life or sexual orientation of the person.

1.4 Sub-processor: Entity (including subsidiaries) designated by the processor with the authorization of the controller to process personal data of the controller.

1.5 Any other term not expressly listed in this clause shall have the meaning set out in Article 4 of the GDPR.

Cyber Guardian

SECOND. PURPOSE

2.1 The purpose of this Annex is to define the conditions under which the Processor will process the Personal Data of the Controller necessary for the proper execution of the Services provided to the Controller, as described in Appendix I to this Annex.

2.2 The personal data of the controller will be processed only for the purpose of providing the contracted services in accordance with the written instructions of the controller set out in this Annex. Where the processor considers it necessary to process the personal data of the controller for a different purpose, he must first request the written consent of the controller. In the absence of such authorization, the processor may not carry out such processing.

2.3 If the provision of the Services involves the collection of personal data, the Processor will comply with the duties of information and responsibility established in clause 5.

THIRD. TYPE OF DATA PROCESSED AND CATEGORIES OF INTERESTED PARTIES

The categories of personal data that the processor will process under this Annex and the categories of data subjects are set out in Annex I.

FOURTH. FUNCTIONS OF THE PARTIES

4.1 In the provision of the services referred to in the Annex, the Processor shall under no circumstances be considered as the Data Controller's Personal Data Controller for any type of processing activity, which may include, among others, the collection , analysis, processing and processing of personal data. the communication or transfer of such data.

4.2 In accordance with clause 4.1 above, the Processor will not under any circumstances include the Personal Data of the Data Controller in its own databases , nor will it use them for its own purposes or other than those established in this Annex and, specifically, in clause 2.

FIFTH. CONSENT TO THE PROCESSING OF PERSONAL DATA

If the processor, in accordance with the instructions of the controller, is required to collect personal data on behalf of the controller, the processor shall fulfill the duties of information and consent collection, monitoring and demonstration set out in the GDPR and provide privacy and data protection notices to the controller for review prior to the collection of personal data.

Cyber Guardian

SIXTH. OBLIGATIONS OF THE CONTROLLER

For the performance of the services, the Data Controller undertakes to make available to the Data Processor the Personal Data and / or the information necessary for the correct processing of the Data for the provision of said Services.

SEVENTH. OBLIGATIONS OF THE PROCESSOR

The Processor undertakes to comply with the following obligations:

2.a To process the personal data of the Data Controller only for the provision of the contracted services, complying with the instructions given in writing by the Data Controller at any time, unless specifically required by the applicable legislation on Data Protection, in which case, the processor shall notify the controller of this legal requirement prior to the processing, unless such notification is prohibited by law for important reasons of public interest.

2.b Maintain its duty of secrecy in relation to the personal data to which it has access, even after the end of the contractual relationship, and ensure that the persons for whom you are responsible have committed in writing to maintain the confidentiality of the personal data processed or are subject to a statutory duty of professional secrecy.

2.c Ensure, taking into account technical progress, implementation costs and the nature, scope, context and purposes of processing, as well as the risk of varying probability and severity in relation to the rights and freedoms of natural persons, that it shall apply appropriate technical and organizational measures to ensure a level of security appropriate to the relevant risk, which may include:

- pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to quickly restore availability and access to personal data in the event of a physical or technical incident;
- a regular process of verification, evaluation and evaluation of the effectiveness of technical and organizational measures, in order to guarantee the safety of the treatment.

When assessing the suitability of the level of security, you must take into account, in particular, the risks posed by the processing of the data, in particular those arising from accidental or unlawful destruction, loss or alteration of the personal data transmitted, store or otherwise process, or unauthorized access or disclosure of such data.

2.d Keep under their control and custody all Personal Data to which the Processor has access for the provision of the Services and not to disclose, transfer or otherwise disclose such Data, including for storage purposes, to persons outside the person in charge of the treatment and the provision of the Services covered by this Annex, without prejudice to the provisions on sub-commission and international data transfers established in clauses 8 and 9 respectively.

2.e Delete or return to the Data Controller, after indicating the Data Controller, all personal data to which he has had access for the provision of the Services. The Processor also undertakes to delete existing copies except where legal provisions require the retention of the personal data of the Controller. However, the processor must keep the data duly blocked, as long as there are responsibilities derived from its relationship with the controller.

2.f Notify the controller without undue delay of any personal data security breaches of which he or she is aware, by providing support to the controller in the notification to the competent data protection authority, and where appropriate, to the data subjects; of security breaches that occur, as well as supporting, where necessary, the conduct of privacy impact assessments.

2.g Notify the controller, without undue delay, of requests for the exercise of rights by the interested parties and assist the controller so that it can comply with the obligation to respond to such requests.

2.h Cooperate with the competent supervisory authority, at the request of that authority, in the performance of its responsibilities.

2.i Make available to the controller all the information necessary to demonstrate compliance with the obligations set out in this Annex, to enable and contribute to audits , including inspections, on the part of the controller or another auditor authorized by him under the agreed conditions. Failure to demonstrate that the processor has correctly complied with the obligations laid down in this Annex shall constitute one of the reasons for the resolution of the Annex.

EIGHTH. SUBCONTRACTING

8.1 The controller expressly authorizes the contracting by the processor of another processor (the " **Subprocessor** ") whose identification data (full company name and NIF) and subcontracted services must be communicated to the Data Controller at least one (1) month in advance of the provision of the service. During this month in advance, the Data Controller may object, in a reasoned manner, to the contracting of the Subprocessor.

8.2 Likewise, the Processor must inform the Data Controller of any planned changes regarding the incorporation or replacement of Subprocessors, thus giving the Data Controller the opportunity to object to such changes.

8.3 The use of the power recognized in the previous paragraph implies the obligation of the Processor to transfer and communicate to the SubProcessor all the obligations arising for the Processor under this Annex and, in particular, the provision of sufficient guarantees regarding the application of the appropriate technical and organizational measures, to ensure the conformity of the treatment with the applicable regulations.

8.4 In any case, access to the data is authorized to natural persons who provide their services to the processor and who act within the framework of the organization of the latter, under a commercial and non-employment relationship. Likewise, access to data is authorized to companies and professionals that the processor has contracted within its internal organizational scope for the provision of general or maintenance services (computer services, consulting, audits, etc.), provided that these tasks have not been arranged by the Processor in order to subcontract with a third party all or part of the Services provided to the Data Controller.

8.5 The Parties acknowledge that the Processor may continue to use those Subprocessors already contracted by the Processor as of the date of this Annex. In any case, the Processor ensures that such Subprocessors (i) comply with the security measures required by the applicable Data Protection legislation and industry or industry standards as of the date of this Annex and (ii) continue to comply with the requirements established for security measures during the duration of the processing activities and this Annex.

NINTH. INTERNATIONAL DATA TRANSFERS

9.1 if the provision of the Services by the Processor requires international transfers of data from data subjects located in the EU to countries outside the European Economic Area (EEA), the Processor shall ensure that he and his Subprocessors have implemented an appropriate mechanism that is recognized by the applicable data protection legislation to allow such data transfers.

9.2 In accordance with clause 9.1 above, the Parties shall sign the standard contractual clauses approved by the European Commission for cases where international transfers of data are foreseen to countries not dependent on the adequacy decision. Such clauses shall govern any international transfer of data to countries outside the EEA. In the event that the competent body or authority updates or otherwise modifies these clauses , or issues a new version thereof, the Parties undertake to sign the most recent version of the applicable standard contractual clauses.

9.3 Where international transfers of data between groups of companies are based on binding corporate rules or any other instrument of a similar nature recognized by applicable data protection legislation, the Data Processor guarantees and ensures that (i) it will maintain and, where appropriate, extend its authorization in the EEA of its binding corporate rules for the duration of this Annex; (ii) notify the processor without delay of any substantial change to that authorization; and (iii) communicate to its Subprocessors any of its obligations under the Binding Corporate Rules, entering into appropriate additional transfer

agreements.

TENTH. RESPONSIBILITIES AND GUARANTEES

10.1 If the Processor or any of its Subprocessors fails to comply with this Annex or any regulation in determining the purposes and means of the processing, the Processor shall be considered responsible for such processing, assuming all responsibilities that may arise for the Processor arising from such breach by the Provider.

10.2 Likewise, both parties agree that the breach of these obligations will be considered grounds for termination of the Annex, so any breach by the Processor, its Subprocessors, employees or persons involved in the provision of the Services on their behalf, will be considered a ground for termination. it will entitle the Data Controller to terminate the Annex and to receive compensation for damages due to the breach of contractual obligations up to an aggregate maximum amount of the compensation received for the provision of the Service (as defined in the General Conditions of Contract) paid by the controller to the processor.

10.3 Where one of the Parties has paid the full compensation for the damages suffered by the processing, that Party shall be entitled to claim from the other Party involved in the processing the part of the compensation corresponding to its share of the liability for the damage.

10.4 If the Processor violates any of the provisions of this Annex or any applicable data protection legislation in determining the purposes and means of the Processing, the Processor shall be considered as a Processor with respect to that Processing.

ELEVENTH. DURATION

11.1 This Annex shall be in force for the entire duration of the provision of the services contracted to the processor. Both Parties agree that the provisions of this Annex, which are expressly or implicitly intended to continue in force after the termination or expiration of this Annex, shall remain in force and shall continue to bind both Parties as stipulated.

11.2 The processing of personal data covered by this Annex shall take place until (i) the Services subject to the General Contracting Conditions no longer require the processing of personal data of the Controller; or (ii) the termination, expiration or termination of the General Conditions of Contract or this Annex.

TWELFTH. APPLICABLE LAW AND JURISDICTION

12.1 This Annex, including all its Appendices, shall be incorporated into the General Conditions of Contract and shall form an integral part thereof.

12.2 This Annex shall be governed by the applicable legislation on Data Protection of Spain and the applicable European, as well as by the resolutions and guidelines of the Spanish Data Protection Agency and other competent bodies in the matter. To resolve any dispute that may arise in relation to the interpretation and / or execution of the provisions of this Annex, both Parties submit to the jurisdiction of the Courts of Madrid, expressly waiving any other legislation or jurisdiction that may correspond to them.

APPENDIX I.

NATURE OF TREATMENT ACTIVITIES

1.I Data categories:

Potential access to any data that may be present on the Customer's devices, including but not limited to:

- Contact details: Include name, surname, email address, phone number and address of users.
- Technical Data: This includes IP address, login data, browser type and version, time zone settings and location, operating system and other technologies of the devices that users use to access the Website.
- Profile Data: Includes the user name and password, and the comments and responses that users include in the Website surveys.
- Usage Data: Includes information about how users use the Website and the products and services offered through it.
- Marketing Data: Includes user preferences for receiving advertising and commercial communications about Cyber Guardian products and services and third parties.
- Cyber security data: Includes data relating to the cyber security of the company to which users belong, which they can share with Cyber Guardian, or which is obtained from third parties.
- Financial data: These include data that users provide on the Website .
- Transactional Data: These include data relating to payments made and the products and services purchased by Users through the Website. If applicable, it also includes questions that they ask us by email or through the chat on the Website.
- Location.
- Email header information, including email addresses, sender name, recipient name, subject, URLs and attachments.
- Occupation, job, employer, relationship with the organization.
- User IP address, user name in Active Directory, mapping in Organizational Unit in Active Directory (conditional if exposed in logs)

- Cloud application accessed by the user (not personal data), activity carried out by the user in the Cloud application (limited to data exchange on interfaces), and name of the user in the Active Directory and / or email alias of third parties with whom data is shared through the Cloud application.

- Personal data collected during the provision of the service and used to provide the service, support and improve the services, including machine events and threat actors data.

- Personal data collected if they are present in unknown or suspicious files that are analyzed for possible malicious activities or vulnerabilities.

- Personal Data collected if the names of employees or contacts are received to respond to Support or Account Management requests.

- Machine event data that could potentially include personal data such as: Device name / unique device identifier, user name, file name, file path, command line, IP Addresses, Unit Name, Group Name, Attributes in Active Directory.

1.II Categories of stakeholders:

Potentially any interested party whose information is present on the Customer's devices, and may include but not limited to:

- Employees of the customer;
- Customers and users of the customer;
- Customer's suppliers;
- Customer Affiliates
- Third parties who relate electronically to the customer.

1.III Types of treatment activities:

- Access;
- Storage;
- Adaptation, alteration or organization;
- Use;
- Recovery;
- Consultation;
- Communication by transmission;
- Restriction, erasure or destruction;
- Collation;

Cyber Guardian

APPENDIX II.

A. MINIMUM SECURITY MEASURES TO BE IMPLEMENTED BY THE PERSON IN CHARGE OF THE TREATMENT

1 **Physical security** .

- Physical barrier controls.
- Identification, registration and accounting of visitors.
- Accompaniment of visitors.
- Electronic access controls (access card) or biometric.
- Video surveillance.
- Guards, security personnel and concierge.
- Alarm and alert procedures.
- Fire detection and extinguishing systems.

2 **Virtual security and data access** .

- User identification and authentication procedures.
- Registration and control of access, modification and deletion of data.
- Password requirements (length, complexity, special characters and password renewal).
- Automatic blocking of the user after a number of failed attempts, password timeout, etc.
- Encryption of passwords and media.
- Encryption of information both in transit and at rest.
- Role-based access and well- established definition of such roles.
- Audit and documentation records.
- Segmentation of customer data in different instances.

3 **Governance and human resources security** .

- Definition and application of standard operating procedures and internal policies regarding the use of personal data throughout its life cycle, including access, manipulation or processing, and secure deletion.
- Control authorization schemes.
- Non-disclosure and confidentiality obligations for employees with access to the controller's personal data.
- Training and awareness about privacy and data protection, including recurring reminders.
- Appointment of a security officer or a data protection officer, as the case may be.
- Audit and risk management of the supplier and/or sub-processor to ensure compliance with applicable privacy and data protection obligations and requirements.

- Identification, documentation and dissemination of the functions and obligations of the personnel of the controller with access to the personal data of the controller.
- Appropriate data classification policies and procedures.
- Definition and implementation of periodic controls in the company, checking, evaluating and evaluating the effectiveness of technical and organizational measures, in order to guarantee the safety of the treatment.
- Disciplinary action against employees who violate privacy and data processing policies and procedures.

4 **Network security, business continuity and availability** .

- Antivirus, EDR, firewalls and routing protocols.
- Exploring vulnerabilities.
- Intrusion detection and prevention systems.
- Encryption of communications and pseudonymization, whenever possible.
- Backup procedures.
- Uninterruptible power supply system.
- Mirror servers.
- Disaster recovery plan.
- Business continuity plan
- Replication of databases and segregation of functions.

5 **Security of the media** .

- Application of an inventory procedure and control of the entry and exit of media and documents.
- Definition of the archiving criteria of media and devices for storage.
- Access control procedure, modification and deletion.
- Labelling of information
- Transport safety.
- Lockable closets .

6 **Security Incident Management** .

- Incident response procedures and policies.
- Recording and accounting for incidents.

7 **Certifications** .

- Maintenance and, where appropriate, extension of the certifications of the processor .

Last update: October 2023