

TERMS AND CONDITIONS

BY CLICKING ON THE "**ACCEPT AND REGISTER**" BUTTON, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD THESE CUSTOMER TERMS ("**CUSTOMER TERMS**").

PLEASE ENSURE THAT YOU READ AND UNDERSTAND ALL OF THESE CUSTOMER TERMS BEFORE YOU START USING THE WEBSITE AND/OR PLATFORM, AS YOU WILL BE BOUND BY THESE CUSTOMER TERMS WHEN YOU CLICK "**ACCEPT AND REGISTER**".

IF YOU DO NOT AGREE WITH ANY OF THESE CUSTOMER TERMS, YOU MUST IMMEDIATELY CEASE ACCESSING AND USING THE WEBSITE AND THE SERVICES BEING PROVIDED UNDER THESE CUSTOMER TERMS. YOUR ACCEPTANCE OF THESE CUSTOMER TERMS WILL OPERATE AS A BINDING AGREEMENT BETWEEN YOU AND CYSECURITY PTE LTD IN RESPECT OF YOUR USE OF THE WEBSITE, AND/OR SUBSCRIPTION OF AVAILABLE SERVICES.

These Customer Terms are between **You ("Customer")**, AND **CySecurity Pte Ltd ("Company"** or **"Cysecurity"**), each referred to individually as **"Party"** and collectively the **"Parties"**.

BACKGROUND

Company owns and operates the website and/or any Application connected to or mentioned on this site and the Services provided under this website. The Website inter alias contains a cloud scan software functionality which enables users to subscribe to such services offered.

These Customer Terms apply to Your access to, and use of, the website and/or its Application (whether through a computer, mobile phone or other electronic device), the subscription services, other services and all information, recommendations and other products and services provided to You on or through the Website.

PARTIES AGREES TO THE FOLLOWING:

The present Terms of Service agreement governs you and/or your Company's (hereinafter referred to as **"Customer"**) usage of one or more software(s) described under **Schedule A** (Hereinafter referred to as **"Software"** in singular or plural) provided by CySecurity Pte. Ltd., Singapore, (**Company**). Company is the sole owner of the Software along with all its associated rights and trademarks. Software is designed to assess and monitor application security and to provide the findings with general remediation guidelines.

1. Term

1.1. The term of this Agreement shall be for the period of subscription and usage by You of the Software offered by the Company.

2. Product And Usage

2.1. The “Software” is designed to provide security assessment, monitoring, and discovery services (hereinafter “**Service**”) for web and mobile applications, and other digital or IT assets (hereinafter "the Infrastructure"). The purpose of the service is to discover vulnerabilities, weaknesses and misconfigurations of the Infrastructure operated and/or owned by the Customer/Third Parties.

2.2. The assessment, monitoring and discovery of vulnerabilities and breaches are only with respect to the following, as applicable: - surface area monitoring (anti-phish, antimalware, trademark, and brand abuse) automated vulnerability Monitoring (discovers vulnerability) - fake mobile application monitoring or rogue app monitoring (to identify fake mobile app). - web search, data breach, dark web - web search (negative news monitoring) - data breach monitoring - dark web monitoring.

2.3. The Customer further provides, on a royalty-free basis, a license to the Company for the usage of the Customers logo which may or may not be the Trademark of the Customer, in connection with any and all marketing activities and promotions or other usage as and when undertaken by the Company. The Customer acknowledges that if such usage is not permitted to the Company, the commercial terms under this Agreement are subject to change as per the Parties discussions.

3. Representations and Warranties

3.1. The Customer understands and hereby accepts that the discovery process may not detect some of its digital assets, related vulnerabilities, misconfiguration, weaknesses or data leaks due to non-reachability of the relevant systems during the discovery process, or the non-intrusive nature of the discovery process, or inability to attribute the asset or data to the Customers/Third Parties with reasonable certainty, or any other circumstances beyond reasonable control of Company. Therefore, Company shall never be liable for any missed or omitted assets, data or information provided to the Customers/Third Parties within the scope of this project.

- 3.2.** The Customer also recognizes that discoveries from the so-called Dark Web, Deep Web and various web and Internet resources is based on Open Source Intelligence (OSINT) meaning that the discovered assets, data and all other information provided to the Customer are already accessible, or otherwise visible or cognizable, on the Internet.
- 3.3.** For the duration of the project, the Customer, grants Company and/or its licensor/s full authority to monitor various web and Internet resources, including so-called Dark Web and Deep Web, on behalf of Customers/Third Parties for which the discovery is being run. The Customer thereby accepts that Company and/or its licensor/s may detect and get Customers/Third Parties data, or data of subsidiaries/affiliates of Customers Third Parties, that has been previously stolen, compromised or leaked. In any case, Company shall promptly bring the relevant data to the attention of the Customer. Company shall never be liable to the Customer or to any third parties for processing or supplying this data. The Customer shall likewise protect and, if necessary, fully indemnify Company for any Customers'/third-party claims related to the discoveries including all legal costs and reasonable lawyers' fee.
- 3.4.** Company takes appropriate measures not to disturb the availability of the Customers' Infrastructure, related systems or network equipment during delivery of the service. Nevertheless, exceptional, unforeseen or unexpected side effects may occur beyond Company's reasonable control, and Company shall never be liable or responsible for any interruptions or slowdowns of Customer's operations, or operations of any third parties related to the Customers and concerned by the assessment, that may occur during the service delivery. The Customers are advised to create a backup of the tested system and data before starting the assessment.
- 3.5.** Company makes their best efforts to identify all possible vulnerabilities and weaknesses within the scope and during the timeframe of assessment. However, Company does not and cannot guarantee that all the vulnerabilities will be detected, and declines any responsibility for missed, undiscovered or unreported vulnerabilities including but not limited to, any data leaks, data breaches, source code leaks or discovery of fake apps.
- 3.6.** The service itself is not intended to prevent, eliminate or fix any vulnerabilities or security weaknesses. The assessment purports to identify vulnerabilities and weaknesses within the Infrastructure, and to propose general remediation solutions for them. The Customer bear the sole responsibility for implementing all necessary corrections for the discovered vulnerabilities and weaknesses. The Customer

understand that vulnerability remediation, proposed consist of general guidelines only, provided “as is” without any warranty of any kind.

- 3.7.** Company'/Company's assessment results reflect the state of security of the Customer Infrastructure only at the time of the assessment's execution, and therefore cannot be considered as permanently up-to-date.
- 3.8.** The integrity of user interface functionality including but not limited to vulnerability management and related features for any types of assessment or discovery projects are provided “as is” without any warranty of any kind.
- 3.9.** Company declines any responsibility for any kind of misuse or unauthorised usage or leakage of any discoveries/findings based on the assessment. The discoveries/findings are provided with strictest confidentiality to the Customer.
- 3.10.** The Customer is strictly prohibited to use Software to test security of any Infrastructure that does not belong to it and/or for which it does not have an explicit, express and undisputed written authorization from the legitimate Infrastructure owner to perform such testing.
- 3.11.** The Customer is not allowed to use Software in countries where the legislation or regulatory rules prohibit such usage.
- 3.12.** In case of violation of the above-mentioned conditions by the Customer, Company reserves the right to immediately suspend the Customer account and refuse any claims for reimbursement, compensation or indemnification for the projects created under this account.
- 3.13.** The Customer unconditionally agrees to use Software only to assess security of the Infrastructure that belongs to it or for which it has an explicit written authorization from the legitimate Infrastructure owner to do so.
- 3.14.** In case of a website security testing, the Customer agrees that an email notification about the assessment may be sent to emails obtained from the website domain WHOIS record, or to the official emails provided directly by the Customer.
- 3.15.** Company also reserves the right to contact the Customer/Third Parties by telephone and by any other appropriate means in order to verify identities and legitimacy to perform assessment of the Infrastructure.

3.16. Company's IP addresses from which the assessment will take place will be communicated to the Customer by email (i) 1 (one) day before the assessment start and (ii) just before the start of the assessment

3.17. The Customer is required to properly authorize or otherwise whitelist Company's IP addresses on its IPS (Intrusion Prevention System), WAF (Web Application Firewall), and any other hardware or software solutions that may partially or entirely block or slow down the assessment and thus influence its completeness and accuracy. Otherwise, accuracy and completeness of the assessment and of its results are not guaranteed by Company. Any claims for reimbursement in such case will be refused.

3.18. The Customer is entirely responsible for accessibility and availability of its Infrastructure during the assessment. If for any reason the Infrastructure will not be fully accessible from any of Company's IP addresses during the assessment, Customer will bear the sole responsibility for incompleteness, inaccuracy or non-delivery of the assessment. Any claims for reimbursement in such case will be refused.

3.19. The Customer must inform and obtain an explicit authorization to perform the assessment from all the third parties (if any) that are directly or indirectly concerned by the assessment. This obligation particularly applies if the Customer are not the sole owner of the web, database or any other servers or equipment where such Customer's Infrastructure or its data are located. Company does not bear any responsibility for delays caused by coordination between the Customer and Third Parties.

4. Obligation to Respect Account Integrity and Confidentiality

4.1. The Customer undertakes to take all reasonable measures to protect its account Credentials from unauthorized third-parties. If the Customer becomes aware of any illegal, unauthorized, unethical or improper usage of its Portal account, it shall immediately inform Company by writing or another reliable and prompt mean.

4.2. The Customer undertakes to be solely responsible and liable to compensate any damages suffered by Company, its employees or agents in case of breach of this clause.

4.3. In the event to Emergencies: The Customer undertakes to provide a valid email and direct phone number in its profile on the Portal, to be contacted in case of emergency (e.g. unexpected event or breach detection). Failure to do so absolves Company from any responsibility and liability in case of unforeseen emergency when interaction with Customer was required to mitigate damages.

5. Measures against certain usage

5.1. In case of any illegal, unlawful, unethical, improper, unauthorized by the present agreement or performed in a bad faith usage of Software, the Customer unconditionally agrees to be solely liable and responsible for any damages suffered by Company including but not limited to direct, incidental and consequential damages and reasonable lawyers' fees, as well as for any liabilities that Company could owe to any third parties in the result of such usage by the Customer.

5.2. In case of any of the above mentioned scenarios, Company retains the right to:

5.2.1. Take any technical measures it deems appropriate;

5.2.2. Inform competent law enforcement agencies;

5.2.3. Inform third parties concerned by the abuse;

5.2.4. Take a legal action against the Customer;

5.2.5. Demand indemnification for all the damages suffered with applicable interest.

6. Methodology of Testing

6.1. The service identifies a range of method phishing and trademark infringement. It further renders only blocking of the actual phishing website by using API thereby making it ineffective. The service detects any trademark infringement and other related brand violations and through the usage of DMCA notice attempts removal of such infringements. The effectiveness of the services mentioned in this clause are purely based on the 3rd Parties.

6.2. The service does not function on websites which are deceptive and similar looking which do not affect any phishing or trademark violation.

7. Limitation of Liability

7.1. In no event shall CySecurity Pte Ltd have any liability to the Customer/Purchaser Parties or to the clients of the Customer (and any Third Parties, if applicable) for any damages whatsoever, including but not limited to direct, indirect, special, incidental, punitive, reputational, regulatory or consequential damages, or damages based on lost profits, cost of procurement of replacement goods or services, lost business, loss of use, loss of or corruption of data, however caused and, whether in contract, tort or under any other

theory of liability, whether or not the Customer/Purchaser Parties (and any Third Parties, if applicable) have been advised of the possibility of such damages. No director or officer of CySecurity Pte Ltd or any of its subsidiaries shall have any personal liability whatsoever to the Customer/Purchaser Parties (and any Third Parties, if applicable).

7.2. Neither Party to the Agreement shall be held responsible, to have failed to meet its obligations under this Agreement, if the delay or the failure in performance on the Agreement is attributable to any cause beyond either of the Party's reasonable control.

7.3. No Third Party Liability. Nothing in this Agreement shall be construed to create any duty to, any standard of care with reference to, or any liability to any person not a Party to this Agreement. There are no third party beneficiaries of this Agreement. Company shall not bear any responsibility or liability for any damages caused by any joint solutions, implementations, or integrations with any third-party technology products of solutions, including but not limited to Web Application Firewalls, DevSecOps tools and SIEMs, that are provided "as is" without any warranty of any kind.

7.4. Upon the Services as described under this Agreement being subscribed to through any intermediary/agent/broker, and not directly through the Company, the Company shall not be held liable and/or responsible for any damages suffered as a result of and arising from the services being subscribed to by the Customer through a third-party intermediary/agent/broker.

8. Confidentiality and Privacy

8.1. Customer Data Protection, Commercial and Business Secrets:

8.1.1. When providing its services under to the present agreement, Company and its employees undertake their best reasonable efforts to handle the information related to, or received from, the Customer/Third Party in a strictly confidential manner and in compliance with security policies and procedures.

8.1.2. All data is accessible only to the authorized Company employees, required to have access this data to perform their direct professional duties..

8.1.3. Company undertakes not to disclose, share or transfer any Customer/Third Party-related data (e.g. technical, operational or vulnerability data) to any unauthorized parties for any purposes, with the only exception when such action is demanded by a valid order of a Singapore court.

8.1.4. The Customer is solely responsible for using Software in accordance with any concerned third party's right to data protection.

9. Termination

9.1. These Customer Terms continues until such time as they are terminated in accordance with this **Clause 9**.

9.2. Either Party may terminate the Agreement prior to expiry of Term of this Agreement if:

9.2.1. In the event of breach by the other Party of any of its Material Provisions under this Agreement, if the said breach is incapable of being remedied within a reasonable period of time, as mutually agreed upon between the Parties;

9.2.2. In the event of breach by the other Party of any of its material provisions under this Agreement including payments, after a notice to remedy such breach within a period of 30 (Thirty) days has lapsed without any resolution;

9.2.3. In the event of the occurrence of a case of Force Majeure continuing beyond a period of 120 (One Hundred and Twenty) days;

9.2.4. In the event of the other Party suffering an Insolvency Event;

9.3. Without prejudice to the rights available to company to terminate the agreement forthwith as enumerated in clause 9.1 and clause 9.2 above, CySecurity may immediately terminate the agreement without assigning any reason by giving to the other a notice in writing by email (hereinafter referred to as "Termination for Convenience"). Advance payments, if any, will be returned within 30 working days by CySecurity subject to pro-rata adjustments for services rendered under the Agreement.

9.4. Effect of Expiration of Term or Termination. Upon any expiration of the Term (subject to a Renewed Agreement or a notice for Renewed Term being issued) or termination of this Agreement:

9.5. Upon termination of these Customer Terms for any reason:

9.5.1. Your rights to use the Website will cease immediately, Your registration and Your Account will cease to apply, and the Company may block Your access to the Website;

9.5.2. The Company will charge You all amounts due and owing at the date of termination and

9.5.3. The Parties must cease acting in a manner that would imply a continuing relationship between the Parties.

9.6. Both Parties shall promptly deliver to the other Party all the Intellectual Property and the Licensed Software (in the Licensee's case) to the other Party and such Party shall continue to retain ownership of such Intellectual Property and the Licensed Software;

9.7. Both Parties shall provide reasonable cooperation and assistance to the other Party in achieving the requisite requirements pursuant to the termination of this Agreement; and

9.8. Both Parties shall (i) return to the other Party, all documents and tangible materials (and any copies) containing, reflecting, incorporating or based on the such Party's Confidential Information; (ii) permanently erase the other Party's Confidential Information from its computer systems; and (iii) certify in writing to the other Party that it has complied with the requirements of this **Clause 9.8.**

10. Miscellaneous

10.1. Entire Agreement: The present agreement constitutes the entire agreement between the Customer and Company with respect to the subject matter thereof and supersedes all and any prior oral and written communications, understandings, promises, arrangements, or agreements relating to such subject matter. The Customer hereby agrees that there are no other representations or warranties relating to the subject matter hereof.

10.2. Severability: If any provision of the present agreement is found to be invalid or unenforceable:

10.2.1. the validity and enforceability of the remaining provisions shall not be affected unless the agreement reasonably fails in its essential purpose; and

10.2.2. such provision shall be replaced by one or more valid and enforceable provisions approximating the original provision as closely as possible.

10.3. Assignment: The Customer may not transfer or assign this agreement, in whole or in part, or delegate any of its duties hereunder, to a third party by change in control, operation of law or otherwise, without the prior written consent of Company. Company

may delegate its duties and assign its rights arising out of the present agreement upon a written notification to the Customer and in case if such transfer of rights will not impact, diminish or negatively affect Customer rights stemming from the present agreement.

10.4. No Third Party Rights: Nothing expressed or referred to in the present Agreement shall be construed to give any person other than the parties to the this Agreement any legal or equitable right, remedy or claim under or with respect to this Agreement or any provision of this Agreement. This Agreement and all of its provisions are for the sole and exclusive benefit of the parties to this Agreement.

10.5. Force Majeure: Company shall be excused from liability for the failure or delay in performance of any obligation under the present agreement by reason of any event beyond its reasonable control including but not limited to Acts of God, fire, flood, explosion, earthquake, or other natural forces, war, civil unrest, epidemic, pandemic, major accident, strike or other labor disturbance, or embargoes.

10.6. Governing Law and Jurisdiction: The present Terms of Service agreement applies worldwide and is governed by and construed in accordance with laws of the Republic of Singapore. Application of any international treaties or conventions is excluded. The Customer irrevocably consents to the jurisdiction and venue of Singapore Courts in connection with any action, suit, proceeding or claim to enforce the provisions of the present agreement, to recover damages for breach of or default under the present agreement, or otherwise arising under or by reason of the present agreement.

SCHEDULE A

The Services provided by the Company shall be based on the Software subscribed to by the Customer. The following Software as services are available and applicable in each or in multiply based on each subscription:

1. **Darwis SFS/ Reejavajra APT Cloud scan:** This is the cloud version Software as a Service. The Software includes SURFACE AREA MONITORING, VULNERABILITY MONITORING, SHIELDSUP SCANNER. Add-ons include dark-web monitoring, data breach monitoring, negative news monitoring.
2. **DARWIS:** This is a Software which runs inside a two virtual machine/KVM on a hardware box, server on the Customer premises. It provides services in relation to DATABREACH, ANTIPHISH AI, ROGUE APP MONITORING, WEBSEARCH (NEGATIVE NEWS MONITORING), INTERNAL VULNERABILITY SCANNER. One virtual machine holds DARW, and another virtual machine holds the internal vulnerability scanner. When DARWIS is activated, DARWIS SFS is activated by default.
3. **Darwis XDT:** This is a Software which runs inside a Virtual machine/KVM on a hardware box, server on the customer premises. It has DATABREACH, ANTIPHISH AI, ROGUE APP MONITORING, WEBSEARCH (NEGATIVE NEWS MONITORING), INTERNAL VULNERABILITY SCANNER. Company uses community edition of open source EDR (END POINT DETECTION AND RESPONSE) combined with backend threat intel for malware signatures. This product includes a honeypot/deception technology. The honeypot traps new viruses and uses the same threat intel API to analyze the malware. If malware is found it informs the EDR to be proactive about the new malware/existing malware. XDT combines power of EDR, deception technology integrated with threat intel API.
4. **IVA – INTERNAL VULNERABILITY SCANNER:** This is a Software that enables internal server/desktop scanning for vulnerability. This scanner uses cloud SaaS logic to scan internal networks.