1. **Definitions**

"**Agreement**" – means these Terms and Conditions and its Schedules.

"**Company**" – means MazeBolt Technologies Ltd.

"**Customer**" – means the entity that purchased Company's Products and Services from Company or from an authorized reseller of Company.

"**DDoS Mitigation Vendor**" – means any Customer which is in the business of providing DDoS mitigation services and/or hardware.

"**Party**" – means either Company or Customer and "**Parties**" means both Company and Customer.

"**Products and Services**" - means the Company's Cyber Security Threat Assessment products and services related to Customer's network, as more fully described in **Schedule A** attached hereto, which are purchased by Customer according to this Agreement.

"**Purchase Order**" means a purchase order by Customer or by an authorized reseller of Company or any other similar document to that effect, which needs to be issued or signed (as the case may be) for the purpose of acquiring the Company's Products and Services.

Capitalized terms which are not otherwise defined herein shall have the respective meanings ascribed thereto in **Schedule A**.

2. **The Services**

2.1 Subject to Customer's payment of all applicable fees, as specified in the Purchase Order, Company agrees to render to Customer: (i) the services properly purchased by Customer in accordance with and subject to this Agreement; and (ii) a non-exclusive, non-sublicensable, nor-assignable, right to use the software included in the services (if any on-site software is deployed) solely for internal use as part of the services.

2.2 Services will commence as follows: (i) in the event that that Customer purchases Traditional DDoS Testing (which may also be referred to as "**Red Team Testing**") or related services – upon receipt of the applicable fees by Company, and (ii) in the event that Customer purchases the DDoS RADAR™ Internal Component and the related Services (as defined in Schedule A), then such Services shall commence upon receipt by Company of a written notice by Customer acknowledging arrival of the said device (if the DDoS RADAR™ Device is purchased) and its installation by Customer. Services shall continue for 12-months intervals, as specified in the Purchase Order, commencing as of the DDoS RADAR™ Internal Component installation at Customer's premises and receipt of the applicable fee by Company, and in any event the 12 months interval shall commence no later than the lapse of 8 (eight) weeks from the issuance of the Purchase Order by the Customer or the signature by the Parties of a similar document to that effect. Renewal of the Services shall be made by the issuance of an additional Purchase Order by the Customer to the Company or the signature by the Parties of a similar document to that effect, as the case may be, all in accordance with the terms hereof.

2.3 **Schedule A** hereto specifies certain limitations and requirements which are applicable to the performance of the Services. Any failure by Customer to fulfill any of the requirements specified in **Schedule A** may result in schedule delays and/or Company's inability to perform the Services and/or Company's ability to successfully commence or complete the Services and/or in additional charges to Customer. Company shall not be required to grant any right herein or provide any services until all due payments are actually received by Company.

2.4 Customer agrees to reasonably assist Company by, inter alia, providing Company access to Customer's sites, allowing network and other technological layouts and providing any information which Company may find necessary from time to time in order to perform the Services, this will include a Company account associated to Customer's account for support services. Customer shall install the DDoS RADAR™ Internal Component independently unless instructed otherwise by Company. Customer shall verify that the DDoS RADAR™ Internal Component and all installed systems are connected to the Internet. In addition, Customer will designate a contact person from its managerial level, who will be available to Company for all coordination and necessary inquiries.

2.5 In the event that Customer implements MazeBolt's PoV (Proof of Value) plan or PoC (Proof of Concept) plan, according to a Scope of Work (SOW) provided (if provided) by MazeBolt and/or offered by MazeBolt via third party sites (such as Google Marketplace), then the terms and conditions in such SoW shall apply, in addition to the terms and conditions herein, and the services provided within the framework of the PoV shall be deemed as Services under this Agreement for all intents and purposes.

3. **Fees**

3.1 As full compensation for Company's performance of the Services, delivery (if the RADAR Device is purchased) and installation of the DDoS RADAR™ Internal Component and performance of Company's other obligations under this Agreement, Customer will pay Company the fees set forth in the applicable Purchase Order.

3.2 Promptly upon receipt of the Purchase Order by Company, Company will prepare and submit to Customer an invoice for the amounts payable for Services according to the Purchase Order. Customer will pay the amount properly due and payable under each of Company's invoices within thirty (30) days after Customer's receipt of the applicable invoice. All invoices will be sent by email to the Customer's point of contact, as designated in writing by Customer.

3.3 Amounts not paid when due pursuant to this Agreement shall bear interest from the due date until actual payment thereof at a rate of 1% per month, or the maximum interest rate permitted by applicable law.

3.4 Except as otherwise specified herein, the fees shall be exclusive of all taxes. Any taxes levied upon this Agreement, the Services and/or the DDoS RADAR™ Internal Component (including the DDoS RADAR™ Device), except for taxes on the income of the Company, shall be borne by the Customer. If the Customer is required to withhold any amounts payable hereunder to the Company, such amount will be so withheld and remitted to the appropriate taxing authority for the benefit of the Company, unless the Company provides the Customer with a certificate of exemption from the appropriate tax authority.

3.5 Any third party costs related to implementation of the DDoS RADAR™ Internal Component will be paid for directly by the Customer, for example: when using a third party provider like AWS (Amazon Web Services), Google (GCP or other services), Microsoft Azure (Cloud services) or VMWare.

4. **Term; Termination**

4.1 This Agreement shall enter into force and effect upon the issuance by Customer to Company of the Purchase Order and shall continue to be in effect until completion of all Services or the earlier termination hereof in accordance with its terms. In parallel to the issuance of the Purchase Order, Company will issue to Customer the MazeBolt Service Agreement Acknowledgement.

4.2 Company shall have the right to terminate this Agreement if Customer breaches a material term of this Agreement, including, but not limited to, nonpayment, and fails to cure such breach within thirty (30) days (ten (10) in the case of nonpayment) after written notice thereof. This Agreement will terminate automatically if Customer: (i) becomes the subject of any voluntary petition in bankruptcy or any voluntary proceeding relating to insolvency, receivership, liquidation or composition for the benefit of creditors, or (ii) becomes the subject of an involuntary petition in bankruptcy or any involuntary proceeding relating to insolvency, receivership, liquidation or composition for the benefit of creditors, if such petition or proceeding is not dismissed within thirty (30) days of filing.

4.3 Termination of this Agreement by Company will be a nonexclusive remedy for breach and will be without prejudice to any other right or remedy of Company. The provisions of Sections 1, 3, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15 and 16 shall survive the termination of this Agreement for whatsoever reason including any other obligation that by its nature survives the termination of this Agreement. Without derogating from the foregoing, solely in the event that Customer has pre-paid for Products for a period exceeding one (1) year, either Party may terminate this Agreement for convenience upon a thirty (30) days prior written notice to the other Party. In this case, Customer that terminates for convenience shall be entitled to receive a refund of 70% of the fees pre-paid by Customer for each full subsequent year of Services remaining, calculated on pro rata basis.

For Example: A Customer that prepays for 5 years and wishes to terminate the Services during the third year will be entitled to receive 70% of the fees paid solely for years 4 & 5, which shall be equal to 70% of the total fees paid by Customer divided by 5, and multiplied by 2.

5. **DDoS RADAR™ Device**. Company shall deliver the DDoS RADAR™ Device to Customer DDU (Incoterms 2010) at the destination designated by Customer. The price of the DDoS RADAR™ Device includes all shipping costs to Customer. Customer shall bear all applicable duties and taxes (including VAT, if applicable). To the extent that MazeBolt pays the applicable duties or taxes, for practical purposes, Customer will reimburse such costs within thirty (30) days of receipt of MazeBolt's invoice. The DDoS RADAR™ Internal component shall be shipped by Company only after Customer confirms in writing to Company that it has received the invoice issued by Company. The DDoS RADAR™ Device will not be sold but leased and title to the DDoS RADAR™ Device shall remain at all times with Company and Customer shall not have any lien or charge over the DDoS RADAR™ Device. Customer shall bear all risk of loss and be solely responsible in respect of the leased DDoS RADAR™ Device until the leased DDoS RADAR™ Device is returned to Company. Company may update the DDoS RADAR™ Device at its own discretion. Upon expiration or termination of the Agreement, Customer shall, at Customer's expense pursuant to Company's instructions, promptly return the leased DDoS RADAR™ Device to Company in the same operating order, repair, condition and appearance as when received, except for normal depreciation and wear and at such address as directed by Company. Until return of the leased DDoS RADAR Device™ to Company, Customer shall be responsible for all storage and for proper and safe custody of the leased DDoS RADAR™ Device. Without derogating from Customer's obligation to return the DDoS RADAR™ Device as described above, if the DDoS RADAR™ Device is damaged or stolen or if Customer otherwise fails to return the leased DDoS RADAR™ Device

to a designated address as notified by Company to Customer in writing, within fourteen (14) days of the termination and/or expiration of the Agreement, Customer shall pay Company Ten Thousand USD (US$10,000). If Customer paid fees for full four (4) consecutive years of Services, title to the DDoS RADAR™ Device for the corresponding Services shall transfer to Customer.

6. **Support Services**. In addition to the Services, Company or its authorized reseller may render Customer certain support services in connection with the Services. In the event that Customer purchases support services, the Service Level Agreement that is attached to this Agreement as **Schedule B** shall apply. In the event that Customer is in a PoC or PoV process or any other process for which no fees have been paid and/or are payable to MazeBolt, then MazeBolt shall use reasonable efforts to perform the applicable obligations pursuant to Schedule B.

7. **Customer's Obligations and Restrictions**.

7.1 Customer shall use the Services and/or the Products solely for its own internal use and shall not (i) copy, reproduce, sell, license (or sub-license), lease, loan, assign, transfer, or pledge the Services and/or the Products, or publicly perform, display or communicate, the Services and/or the Products, or otherwise use the Services and/or the Products in a time-sharing, outsourcing, or service bureau environment or otherwise permit any third party to do any of the foregoing; (ii) modify, disassemble, decompile, reverse engineer, revise or create any derivative works of the Services and/or the Products or attempt to access or discover its source code; (iii) use the Services and/or the Products for any type of benchmarking, competitor analysis, product enhancement and/or similar activities; (iv) ship, transfer, or export the Services and/or the Products or use the Services and/or the Products in any manner that is prohibited by law, including without limitation, to sell, distribute, download or export the Services and/or the Products: (a) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Lebanon or Syria, (b) to anyone on the U.S. Commerce Department's Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals, (c) to any country to which such export or re-export is restricted or prohibited, or as to which the U.S. or Israeli government or any agency thereof requires an export license or other governmental approval at the time of export or re-export without first obtaining such license or approval, or (d) otherwise in violation of any export or import restrictions, laws or regulations of the U.S. or Israel or any foreign agency or authority. Customer agrees to the foregoing and warrants that it is not located in, under the control of, or a national or resident of any such prohibited country or on any such prohibited party list; (v) contest Company's intellectual property rights to the Services and/or the Products; (vi) remove or add any labels, notices or logos to the Services and/or the Products, (vii) use the Services and/or the Products to initiate, aid, participate, direct, or attempt to attack, hack or crack, or to send destructive or potentially harmful contents to any device, whether those devices are owned by Company and/or by any third party and/or otherwise use the Services for any illegal act or purpose; (viii) circumvent, disable or otherwise interfere with security-related or technical features or protocols of the Services and/or the Products, such as features that restrict or monitor use of the Services and/or the Products; or (ix) cause or permit any third party to do any of the foregoing.

7.2 Without derogating from the foregoing, in the event that Customer (i) has any type of DDoS service offering, or (ii) if Customer generates revenue from DDoS service offering, or (iii) if the Customer is a DDoS mitigation provider, or (iv) if Customer is a DDoS testing or stress testing provider, or (v) if the DDoS RADAR™ Internal Component is being used to fine tune and/or to analyze the DDoS protections of any of Customer's customers, then Customer shall not be entitled to utilize the DDoS RADAR™ Internal Component other than for its internal use only and not for the benefit of any of its customers, either by way of resale, by adding networks of other organizations or in any other way that circumvents the limitations on this Agreement, unless Customer obtains Company's approval for such specific uses in advance and in writing. In the event that Customer wishes to utilize the DDoS RADAR™ Internal Component for any purpose, other than for internal use, Customer shall notify Company in writing and specify the requested uses in reasonable detail. Company shall have the right to either approve or reject Customer's request, in Company's sole discretion. Customer acknowledges that any additional use of the DDoS RADAR™ Internal Component that it may request from Company will entail the payment of additional fees to Company, as agreed between the Parties.

7.3 Customer is prohibited from publishing in any manner reports or reporting data provided to it within the framework of the Services, unless Customer obtains the prior written approval of Company. If approval is so granted by Company, Customer shall publish only the full report as-is (and not partial information) and may add preliminary wording that will be provided by Company, and no other wording or information. In addition to the foregoing, Customer shall not disclose any such report to a third party mitigation provider unless it first executes with such third party a confidentiality agreement to ensure the confidentiality of the report, and Company may request Customer to provide it with a copy of such signed confidentiality agreement.

8. **Representations and Warranties**

8.1 Customer represents and warrants that (i) it is the owner of or has full power and authority to all IT infrastructure, IP addresses, Network address spaces (e.g. 192.168.22.0/24) and FQDNs (Fully Qualified Domain names) provided to Company to support the Products or any additional IP addresses, Network address spaces (e.g. 192.168.22.0/24) and FQDNs (Fully Qualified Domain names) which may be added through the Company's platform during the use of Products; (ii) all information provided by Customer is accurate and Customer is permitted to use and/or divulge such information to Company in connection with the Services; and (iii) Customer has clarified the technical requirements of the Products with Company and is satisfied that the technology of the Products can work in the topology described by Customer to Company.

8.2 Each Party hereby represents and warrants to the other that: (a) it has all requisite corporate rights, power and authority to execute, deliver and perform its obligations and undertakings under this Agreement; (b) this Agreement has been duly executed and is enforceable against such Party in accordance with its terms; and (c) there is no legal, contractual or other impediment to its entering into this Agreement and the performance of its obligations hereunder.

9. **Confidentiality**. Each Party agrees to keep confidential and to use only for purposes of performing its obligation under this Agreement, any proprietary or confidential information of the other party disclosed pursuant to this Agreement which is marked as confidential or is identified at the time of disclosure as confidential or which would reasonably be considered confidential or proprietary in nature. The obligation of confidentiality shall not apply to information which is publicly available through authorized disclosure or which is required by law, government order or request to be disclosed (provided that the receiving party shall give written notice to the other party prior to such disclosure and an opportunity, at the objecting party's expense, to take legal steps to resist or narrow such request). Upon any termination of this Agreement, each Party shall return to the other party all confidential information of the other Party, and all copies thereof, in the possession, custody or control of the party unless otherwise expressly provided in this Agreement. This provision shall survive the termination or expiration of this Agreement for any reason.

10. **Intellectual Property**. All right, title and interest, including all intellectual property rights, in and to the Company's website, software, Products and the Services and any enhancements, improvements and derivatives thereof are and shall at all times remain the sole and exclusive property of Company. Customer acknowledges that no title or license is granted hereunder with respect to Company's intellectual property rights.

11. **Disclaimer**

11.1 THE PRODUCTS AND ANY RELATED SERVICES ARE PROVIDED "AS IS", WITHOUT ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED. TO THE MAXIMUM EXTENT PERMITTED BY LAW, COMPANY DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE, SECURITY AND NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE PRODUCTS AND ANY RELATED SERVICES REMAINS WITH CUSTOMER.

11.2 COMPANY DOES NOT WARRANT THAT THE PRODUCTS AND ANY RELATED SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE; OR THAT ERRORS/BUGS ARE REPRODUCIBLE OR THAT ERRORS/BUGS ARE REPAIRABLE AND DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE PRODUCTS AND ANY RELATED SERVICES IN TERMS OF THEIR CORRECTNESS, USEFULNESS, ACCURACY, RELIABILITY, OR OTHERWISE. CUSTOMER SHALL BE RESPONSIBLE FOR TAKING ALL PRECAUTIONS CUSTOMER BELIEVES ARE NECESSARY OR ADVISABLE TO PROTECT CUSTOMER AGAINST ANY CLAIM, DAMAGE, LOSS OR HAZARD THAT MAY ARISE BY VIRTUE OF ANY USE OF OR RELIANCE UPON THE PRODUCTS AND ANY RELATED SERVICES AND FOR VERIFYING ANY OUTPUT RESULTING FROM USE OF THE PRODUCTS AND ANY RELATED SERVICES.

12. **Limitation of Liability**

12.1 NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE TO BUSINESS EARNINGS, LOST PROFITS OR GOODWILL AND LOST OR DAMAGED DATA OR DOCUMENTATION, SUFFERED BY ANY PERSON, ARISING FROM AND/OR RELATED WITH THIS AGREEMENT, EVEN IF SUCH PARTY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL EITHER PARTY'S TOTAL LIABILITY UNDER THIS AGREEMENT OR AS A RESULT OF THE PRODUCTS AND ANY RELATED SERVICES EXCEED THE AGGREGATE FEES ACTUALLY PAID FOR THE PRODUCTS AND SERVICES BY CUSTOMER.

12.2 NOTWITHSTANDING THE FOREGOING, NOTHING HEREIN SHALL LIMIT EITHER PARTY'S LIABILITY FOR WILLFUL MISCONDUCT, BREACH OF SECTION 8.1(i) ABOVE, MISAPPROPRIATION

OF COMPANY'S INTELLECTUAL PROPERTY RIGHTS OR BREACH OF CONFIDENTIALITY OBLIGATIONS.

12.3 WITHOUT LIMITING THE FOREGOING, IT IS SPECIFICALLY UNDERSTOOD AND AGREED THAT WITHIN THE FRAMEWORK OF THE PRODUCTS AND ANY RELATED SERVICES, COMPANY WILL INTENTIONALLY CAUSE DISRUPTIVE TESTS TO CUSTOMER'S NETWORK, DURING SIMULATED ATTACKS, AND COMPANY WILL NOT BE LIABLE FOR ANY: (A) NETWORK DOWNTIME, (B) DAMAGED EQUIPMENT, (C) FINANCIAL LOSS WITH RESULTS FROM THE PRODUCTS AND ANY RELATED SERVICES, OR (D) IDENTIFYING AREAS OF WEAKNESS IN THE NETWORK AND PATCHING THEM. CUSTOMER SHALL HAVE SOLE LIABILITY AND RESPONSIBILITY FOR DOWNTIME AND LOSS OF DATA TO THIRD PARTIES WHO RELY ON OR INTERFACE WITH CUSTOMER'S SYSTEMS. **IN NO WAY COMPANY GUARANTEES A REAL DDOS ATTACK, PHISHING ATTACK, MALWARE ATTACK OR ANY OTHER CYBER ATTACK WILL NOT TAKE DOWN, EXPLOIT, STEAL DATA OR DAMAGE CUSTOMER'S NETWORK.**

13. **Force Majeure**. Neither Party shall be deemed to be in breach of this Agreement, or otherwise be liable to the other, by reason of any delay in performance, or non-performance, of any of its obligations hereunder to the extent such delay or non-performance is due to circumstances beyond its reasonable control, provided that such Party shall promptly notify the other Party of the occurrence thereof.

14. **DDoS Mitigation Vendor**. In the event that Customer is in any way considered a DDoS Mitigation Vendor, or is a vendor of any other type of DDoS assessment or testing activities, then the following provisions shall apply to it:

    (i) Customer hereby acknowledges that the Company's business is in the field of cyber threat assessment, and as such, the Company has independently performed, and will continue to perform after the date hereof, various tests and ongoing research activities related to its technology in other environments and may obtain, in the course of such research, certain information regarding the Customer.

    (ii) Customer hereby agrees that the information mentioned in sub-section (i) above shall not be deemed as confidential information of Customer for the purposes of this Agreement.

    (iii) Customer further agrees that the Company shall be entitled to publish the results of any tests and research independently performed thereby as aforesaid and use it for any other purpose within its business activities, and Customer acknowledges that the Company is vendor-neutral as of the time of these Terms and Conditions being agreed upon by Customer.

    (iv) Customer shall be entitled to use the reports issued by the Company in course of rendering the Services for *internal purposes only*. In furtherance of the foregoing, Customer shall not be entitled to publish or otherwise make public any such report or other data obtained in the course of the performance of the Services, unless Customer first obtains the prior written consent of the Company, duly signed by Company's authorized representative.

    (v) Customer shall not be entitled to disclose the nature of this Agreement and its existence as well Customer's engagement of MazeBolt, unless Customer first obtains the prior written consent of the Company, duly signed by Company's authorized representative.

15. **Notices**. Any notice given by one Party pursuant to this Agreement shall be in writing and delivered by hand or by mail or facsimile to the addresses specified below for that purpose, unless a Party notifies the other Party in writing about a change in its address. Any notice delivered by hand shall be deemed to have been received upon delivery, any notice delivered by facsimile shall be deemed to have been received on the first business day following the day it was sent and if delivered by post it shall be deemed to have been received seven (7) days after posting by prepaid registered airmail.

Company:

MazeBolt Technologies Ltd.
7 Jabotinsky Street
Moshe Aviv Building
Ramat Gan, Israel
Attn: Matthew Andriani
Title: CEO

Customer: as set forth in the Purchase Order.

16. **Miscellaneous**. This Agreement shall be governed exclusively by and construed in accordance with the applicable laws of the State of Israel, excluding its conflict of law rules. The Parties hereby agree that the competent courts of Tel Aviv-Jaffa shall have the sole jurisdiction regarding any dispute that shall arise between the Parties under this Agreement and each Party hereby submits itself to the exclusive jurisdiction of these courts; Contractor is an independent contractor, and is not an employee, agent, joint venturer, or partner of Company. Nothing in this Agreement shall create any agency, partnership or joint venture between the Parties. Neither Party shall act or describe itself as the agent of the other Party nor shall it represent that it has authority to make commitments on

behalf of the other Party; Company may identify Customer as a customer of Company in press releases and marketing materials, and in demonstrations and presentations. Identifying Customer as customer as permitted by this Section may include using Customer's name, referring to the existence of this Agreement and/or using an exact copy of Customer's corporate logo to identify Customer on Company's website, blogs and marketing materials; This Agreement and its Schedules constitute the entire agreement between the Parties with respect to the matters set forth herein, and replaces and cancels any previous negotiation, agreement or contract concerning these matters; In the event of a contradiction or inconsistency between the terms and conditions of this Agreement and the terms and conditions for a Schedule hereto, the terms and conditions of the Schedule shall prevail. Any terms and conditions set forth in an Order Form that amend or modify the terms herein shall supersede and dominate over the terms of the Agreement or a Schedule; No modification and/or amendment to this Agreement shall be valid unless made and approved in writing by both Parties; Neither Party shall have a right to set off any amount against the payments applying to such Party hereunder, for any reason whatsoever; No waiver, delay in acting or extension on the part of either Party shall be deemed to be a waiver of its rights hereunder and/or under any law, nor shall they serve as a basis for a claim, unless such waiver is made explicitly and in writing.

SCHEDULE A

General Description and Technical Requirements of Company Product and Services

1. **MazeBolt Platform**

The MazeBolt Platform is a web-based cyber security apparatus that validates organizations' cyber security defenses, through automated and ongoing threat assessment modules. MazeBolt Platform **evaluates defenses** to DDoS Attacks through 2 validation modules providing DDoS threat assessment:

(i) DDoS RADAR™ Simulation Module (Next Gen. DDoS Mitigation), as per an annual license purchased from the Company; and

(ii) Red Team DDoS testing module (Disruptive DDoS Testing), which can be purchased in addition to the relevant license acquired by a Customer.

2. **License to the MazeBolt Platform**

2.1 Company provides annual licenses pursuant to which Distributed Denial of Service (DDoS) Simulations will be performed against both Cloud based and the Internal network infrastructures. **Company only provides legitimate simulation "network traffic" generated from nodes from the major cloud providers distributed globally.** These are the types of DDoS Simulation solutions that are included in the licenses that the Company grants **DDoS RADAR™ – Next Gen. DDoS Mitigation**

2.1.1 DDoS RADAR™, is a technology which runs both from Company data center, coupled with a co-ordination device hardware provided by MazeBolt or Customer VM at the Customer data center (a "DDoS RADAR™ Internal Component") to provide DDoS vulnerability assessments and network health monitoring.

2.1.2 The DDoS RADAR™ module has a Non-disruptive DDoS validation methodology which should not disrupt network operation while running.

2.1.3 DDoS RADAR™ automatically scans networks provided, for new targets, and then validates those targets for DDoS vulnerabilities.

2.1.4 DDoS RADAR™ runs in an ongoing continuous manner to identify DDoS vulnerability in Customers' data center services.

2.1.5 The DDoS RADAR™ continuously runs at scheduled period of time DDoS attacks to see how Customer DDoS defenses are working and provides a result of "PROTECTED" or "PARTIALLY PROTECTED" or "VULNERABLE" (varying other metrics may be provided). Customers can use these metrics to strengthen their infrastructure to DDoS attacks.

2.1.6 The following are requirements for the DDoS RADAR™ to work in every Customer's network environment. If during the term of the license acquired by the Customer the network environment no longer supports any of the following requirements, then the license will immediately terminate, and no refund will be provided to Customer:

2.1.6.1 Customer is required to place the DDoS RADAR™ Internal Component in Customer Data center, downstream (after) various DDoS protection apparatus deployed, in Customer's data center(s). The DDoS RADAR™ Internal Component is required to be deployed by Customer on a TAP (Mirror) port (likely in the DMZ) of Customer environment and able to access all traffic being passed to Customer's external facing servers IP addresses on a TAP (Mirror) port. Company must be able to see its own originating, original, source IP addresses of its attack simulation nodes, which generates traffic towards targets at the Customer. Currently a maximum of 4 mirror ports is supported per DDoS RADAR™ Internal Component.

2.1.6.2 Each physical data center requires a dedicated DDoS RADAR™ Internal Component setup.

2.1.6.3 DDoS RADAR™ can only validate DDoS mitigation systems for which it is deployed downstream to and being protected by at the time of validating that system. DDoS RADAR™, additionally requires its TAP (Mirror) port to see all traffic from Company IP's (Original sources) towards Customer external facing IPs (seen by anyone on the internet), being validated to DDoS attacks.

2.1.6.4 Company cannot check any technical setup, whereby Company cannot see its own simulation or scanning source IPs. Customer understands this and is aware of this and acknowledges that its technical setup and intended place of deployment will allow Company to see its original simulation and scanning source IP's. The DDoS RADAR™ requires that it can read the simulation and scanning node original source IP's from Company's cloud component of DDoS RADAR™, it is up to Customer to ensure that DDoS RADAR™ on premise component can see the original scanning node source IP's. If the DDoS RADAR™ is deployed downstream from a

CDN it is a requirement that the DDoS RADAR™ Internal Component can see cleartext HTTP traffic in order to validate the CDN DDoS mitigation capabilities.

2.1.6.5 Permanent Geo-IP blocking as part of Customers DDoS mitigation policy may not be supported by the DDoS RADAR™ technology or special requirements may need to be implemented at an additional cost to Customer.

2.1.6.6 Customer acknowledges reading Company's latest installation guide and has understood that DDoS RADAR has technical compatibility with Customer's environment/s, Customer has completed its due diligence with the relevant technical personnel on Customer's side and held any relevant discussions with Company to clarify any areas of uncertainty.

2.1.6.7 Company requires a management port is setup for the DDoS RADAR™ Internal Component, this management port requires port 443 (HTTPs) to be open for outgoing communication with the cloud component on all intermediary security devices (e.g. firewalls).

2.1.6.8 The DDoS RADAR™ Internal Component supports up to **500Mbps** of DDoS simulation traffic. A combined rate of simulation traffic and concurrent normal customer traffic, may not exceed 10Gbps, combined rates exceeding 10Gbps are not supported by DDoS RADAR™ Internal Component.

2.1.6.9 Company at an agreed upon schedule, will regularly port scan for new services and targets in the defined network. These services and targets will be checked for DDoS vulnerabilities.

2.1.6.10 The DDoS RADAR™ will run non-disruptive attack simulations against the targets on an agreed upon predefined schedule. These targets are either manually or automatically (through port scans) added by Company.

2.1.6.11 The Company has designed the DDoS RADAR™ to be non-disruptive to ongoing production systems of Customer. For this Company requires Customer to run the DDoS RADAR™ in a manner laid out by Company, this will entail an initial period where the DDoS RADAR™ runs at a lower rate, validating that there are no fundamental flaws in Customer's IT infrastructure or services. This period will last as long as it takes for Customer to solve such deficiencies in the IT infrastructure or network services, thereby avoiding any disruption to Customer services.

2.1.7 Company's DDoS RADAR™ is continuously updated to meet evolving threats from hackers and by default has over 100 attack types tests are included, covering, layer 3, 4 and 7 DDoS attacks.

2.1.8 Customer agrees that Company will be authorized to perform regular port scanning and DDoS simulations against networks specified by Customer through the account setup phase with Company.

2.1.9 Customer understands that if a target IP identified does not have a service and cannot be monitored (E.g. HTTP, HTTPs, SMTP etc.), then the DDoS RADAR™ cannot validate that target IP.

2.1.10 DDoS RADAR™ will not begin to provide reporting on DDoS vulnerabilities found until DDoS RADAR™ Internal Component is deployed and configured as required in line with Schedule A & Schedule B of the Agreement. Customer will have to access to continuous real-time reporting of the DDoS validations. All reporting for DDoS RADAR™ is accessed via the MazeBolt Platform and is provided as is. In addition, Customer will have access, within the framework of the license, to quarterly executive high-level reports highlighting the DDoS vulnerabilities identified and progress in DDoS Gap management.

2.1.11 The license offered by the Company also includes professional services (support and vulnerability remediation consulting services).

2.1.12 **DDoS RADAR™ features available through the MazeBolt Platform UI (this is subject to change at anytime and fully at the discretion of Company) –**

Module	**Limitations**
Reporting of DDoS RADAR™ Next Gen. DDoS mitigation. With access to real-time reporting via MazeBolt Platform.	• The DDoS RADAR™ license will determine the scope of the targets that will be evaluated in Customer environment. • Non-Disruptive DDoS Simulations are up to 500Mbps and up to 2500 hours annually, of DDoS RADAR™ runtime (unless otherwise specified).

2.2 **Red Team Baseline DDoS Testing Cycles (Additional feature on top of the standard RADAR™ license)**

The BaseLine DDoS Testing Cycle	**Red Team DDoS Simulation**	A 3-hour long testing session that includes 18 DDoS attack vectors from layers 3, 4 and 7 (See Figure 1 for details) that will provide Customer with a detailed report of the human and response handling, as well as the vulnerabilities identified in their DDoS mitigation posture.

2.3 **Red Team Bandwidth Test Simulation (Additional feature on top of the standard RADAR™ license)**

High Bandwidth 'Clip on'	A 15 minute high bandwidth test @ 50Gb for the following three volumetric DDoS attack vectors: UDP Flood, UDP Garbage Flood, Empty Connections Flood ***Note * The 'Clip-on'** is only available for 20Gb BaseLine tests or for Customers with DDoS RADAR™ already working in the Customer's environment.

SCHEDULE B

1. Service Level Agreement - DDoS RADAR™ Service – Platinum "Support Level"

Company, or its authorized reseller, as the case may be, will render the following **Support Services** for DDoS RADAR™ services acquired by Customer within the platinum support package.

1.1. **Bug Resolution** – Company will investigate any suspected bug reported to us by Customer.
1.2. **Validation Scheduling Approval** – All DDoS RADAR™ ongoing test scheduling will be confirmed with Customer prior to scheduling. Or Customer may schedule testing independently.
1.3. **Account management introduction** – Customer will be entitled to a single account management introduction call lasting up to 90 minutes. This call will focus on the annual DDoS validation strategy. MazeBolt will use best commercially reasonable practice to schedule such a call within 3 working days from Customer request.
1.4. **DDoS RADAR™ Internal Component Troubleshooting –** DDoS RADAR™ Internal Component requires a single internal IP and to communicate to external networks. Additionally upon request, Company may request Customer on a temporary basis remote connectivity to DDoS RADAR™ Internal Component \ console.
1.5. **DDoS RADAR™ Internal Component Deployment –** DDoS RADAR™ Internal Component is required to be deployed by Customer on a TAP (Mirror) port in the DMZ of Customer environment. Customer will provide Company correct rack space and location for deployment. Any hardware issues with the DDoS RADAR™ Device has an SLA of 3 working days for repairs. Customer will provide reasonable physical access or remote access to the DDoS RADAR™ Device to Company or Company's OEM provider, as required to maintain, troubleshoot or replace the DDoS RADAR™ Device when needed, any delays by Customer for access to hardware will delay repairing of deployed hardware. Unless otherwise specified Customer must deploy hardware in its datacenter without Company physically onsite, though Company will provide support to Customer in the deployment phase.
1.6. **Ongoing account management** – Customer will be entitled to a quarterly account management call of up to one hour. The purpose and scope of this call will be to improve the DDoS testing and analyze past tests as well as scheduling future tests.
1.7. **Reporting –** Company will provide Access to reporting via Company platform. All reporting is provided as is. Company will provide a quarterly "Executive report" and Customer may export a "Vendor Report" independently at any time. All reporting is provided via the MazeBolt Platform.
1.8. **Correspondence via email or product** – Support queries will be addressed via email or product platform. Customer will also be provided a support phone number, which will be available during normal working hours.
1.9. **Corresponding with DDoS mitigation vendors** – Company will assist Customer with communication with DDoS mitigation vendor with regards to vulnerabilities identified. Company will be copied on emails with both Customer and 3rd party mitigation vendors together with the Customer, however Company will not directly communicate with the mitigation vendor without Customer's involvement at all times.
1.10. During the course of Support, Professional services or Account Management, Company may divulge opinions on 3rd party vendors or other technical or procedural setups. All such information is based on Company's expertise and experience and is divulged as is without Warranty or additional support.
1.11. **Escalation Path** – Customer will be provided an escalation path in the event of account management or support not being satisfactory. Together with an Escalation Contact.
1.12. **Support Hours** – Customer will be eligible for up to 20 support hours annually from Company.
1.13. **Response time** – 1 working day.

Support Coverage – Traditional DDoS Validation:

Company will render the following **Support Services** for Traditional DDoS testing acquired by Customer within the platinum support package.

1.14. **Bug Resolution** – Company will investigate any suspected bug reported to us by Customer.
1.15. **Test plan Approval** – No DDoS test is run prior to a test plan being approved by Customer. If Customer requires a clarification with respect to a test plan Company will reply to Customer by either email or by contacting the Customer by phone, using the phone number provided by the Customer.
1.16. **Account management introduction** – Customer will be entitled to a single account management introduction call lasting up to one hour. Call scheduling may take up to 3 working days.
1.17. ***APT DDoS testing (Where applicable)** – If Customer is performing APT DDoS testing, Company may provide additional temporary incoming call support or account management for the duration of the testing. Company will inform the Customer of the customized process if required, as well as the duration of any such support. Company may stop or start this temporary support as it sees fit and it is only applicable to APT DDoS testing.
1.18. **Reporting –** Company will provide access to reporting via the MazeBolt Platform. Reporting is provided as is.

1.19. **Correspondence via email or product** – Support queries will be addressed via email or product platform.
1.20. **Support Hours** – Customer will be eligible for up to 6 support hours annually from Company.
1.21. **Response time** – 3 working days.

2. General Services Level Agreement

These General Terms together with their appendices represent the Service Level Agreement between MazeBolt Technologies Ltd. ("Company") and Customer for the provision of support services ("Support Services") in connection with the products and services purchased by Customer pursuant to the Purchase Order issued by Customer and Company's Terms and Conditions ("Agreement").
The Support Services shall be rendered by Company or its authorized reseller, as the case may be, to Customer in accordance with the Service Level Agreement. It is hereby agreed as follows:

2.1. **Support, Professional Services or Account Management** – For the purposes of these General Terms, the terms "account management", "support" and "Professional Services" shall be used in the same context.
2.2. **Support Eligibility** - Only Customers who purchased **annual services** according to a Purchase Order and the Company's Terms and Conditions will be eligible to receive the Support Services by the Company is accordance with the Service Level Agreement.
2.3. **Contacting Support** – Support may be contacted either via support@ mazebolt.com or Company product interfaces or telephone support where applicable and based upon Support Level purchased. Company may, at its discretion, assign a support ticket number depending on the issue.
2.4. **Support Level** – Company offers three support levels for each service purchased by a Customer – bronze, platinum and gold. Each support level affords different response times and involvement by the Company support staff. Customer shall select the support level that it wishes to acquire concurrently with the issuance of the Purchase Order to the Company.
2.5. **Information and Co-operation by Customer** – In order for the Company to successfully perform the Support Services, Company may require Customer to fully and timely cooperate in the support process and provide Company with the necessary information, as requested. Lack or delay of co-operation by Customer may render Company unable to resolve a support issue or severely delay the resolution times.
2.6. **Response Time** – Is the time in which Company will respond by email to Customer's inquiry. Response time does not guarantee resolution of the support issue.
2.7. **Clarity of Support Coverage** – Customer is requested to present any question or ambiguity with respect to the support coverage offered by Company prior to the execution of the Service Level Agreement. Following the execution of the Service Level Agreement, any question or ambiguity shall be resolved by Company.
2.8. **Support Hours** – The amount of cumulative time that will be invested by Company in all activities defined in the support level or otherwise provided to Customer by Company to perform Company services. Support hours are utilized and accumulated through activities which may include, for the sake of illustration and without limitation:
  2.8.1. Account management Calls or emails
  2.8.2. Support calls or emails
  2.8.3. Back office work by Company
  2.8.4. Additional reporting requested
  2.8.5. Reviewing of vulnerabilities
  2.8.6. Communication with 3rd party vendors
  2.8.7. Customer branding/Customized branding
  2.8.8. Assisting of troubleshooting technical issues
  2.8.9. Customer training
2.9. **Measurement of Support hours** – The time invested by Company in the rendering of Support Services shall be measured in no less than half an hour (30 minutes) increments.
2.10. **Support Hours Recording** – Company will record internally the actual time invested in the rendering of the Support Services to Customer. Company will inform Customer once the quantity of support hours purchased thereby has been exhausted.
2.11. **Bug Resolution** – Company does not guarantee the resolution of bugs nor the amount of time which will be required to resolve certain bugs. Customer should contact support to begin suspected bug investigation.
2.12. **Feature Requests** – Any new or additional feature requested by a Customer will be added by Company subject to Company's prior consent. Company cannot guarantee the implementation of any new or additional feature and/or the time schedule therefor.
2.13. **IPs Defined** – Whether for DDoS RADAR™ or DDoS testing or any other module, IPs defined indicates a particular network host or service. For DDoS RADAR™ IP's defined will be done through the MazeBolt Platform UI.
2.14. **Support Language** – All Support Services shall be provided by Company in English only.

2.15. **No Accumulation of Support Hours** – The support hours purchased by a Customer per each period of time specified in the Service Level Agreement will not be accumulated to the subsequent period of time. For example: If Customer purchased 6 hours of support per annum, and used only 3 hours during such year, the 3 unused support hours shall not be accumulated to the next year and the quantity of support hours for the next year shall be 6 hours.

2.16. **Unreasonable Support Queries** – If Company determines that Customer is initiating an unreasonable amount of support queries, Company may inform customer that support usage has been consumed and additional support may need to be purchased.

2.17. **Scope of Company Support Coverage** – Company will support only its own products, services and methodologies related to its products and services. Even though in some cases Company may give information related to 3rd parties, it is understood that Company does not support in any way Customer's systems or any third party's appliances, systems, software etc. Other activities which are not covered by Company's support, include, for the sake of illustration and without limitation:

- 2.17.1. CSV generation or creation at Customer
- 2.17.2. Whitelisting
- 2.17.3. Email box setup
- 2.17.4. Device configurations of third party devices
- 2.17.5. Understanding mitigation mechanisms of third party software or devices
- 2.17.6. Network troubleshooting
- 2.17.7. Server or software troubleshooting

2.18. **Expected Environment** – The implementation of Company's products and services may require specific requirements on the Customer's IT infrastructure. Company will inform the Customer of such requirements where needed. Customer shall be solely responsible for the implementation of such requirements in a timely manner and any delay in the implementation of such requirements may further delay the execution of the project for the Customer. Company shall in no way be responsible for such delays. For example, but not limited to and only for the sake of illustration: Whitelisting an IP address for a phishing mails or RADAR™ monitors towards the Customer environment. Company will inform Customer in advance (or at such a time as it becomes required) of the IP address or addresses, which need to be whitelisted. Customer shall be solely responsible for the implementation of the whitelist for any purpose, including for the proper functionality of the DDoS RADAR™, without any support from Company. Any significant delays or troubleshooting caused to Company due to inadequate expected environment may require additional support by Company for an additional fee to be paid by Customer.

2.19. **MazeBolt Platform Support** - Company will investigate any suspected bug reported to Company by Customer for general issues. The response time will be in accordance with the selected support level.

2.20. **Additional Support** – Any additional support required by Customer will first be approved by Company and Customer. Company will require Customer to issue a purchase order or a similar document to that effect for the purchase of such additional support, and may also require payment therefor prior to performance of the additional support services. Any additional support services purchased by Customer shall be subject to the Service Level Agreement and shall be deemed as part of the Support Services.

2.21. **Suspension or Termination of Support** - Company reserves the right to suspend the Support Services in the event of non-payment, partial payment or late payment for such services.

2.22. **Normal Working Hours** – Sunday through Thursday, 9am to 5pm (Israel Standard Time).

2.23. **Escalation Contact** – Some support levels may include an escalation contract. The contact is provided for emergency situations only and is intended when allocated account manager or support query is not progressing as expected. Prior to using the escalation contact, the support and account management contacts should have already been contacted by Customer. Company will be entitled to refrain from responding to a support query which does not seem urgent and may be handled in the regular support channels and/or require payment of additional support fee in such cases. Prior to taking any such an action, Customer will be issued an official warning about overusing emergency contact. In such case, Company may also cease any Support Services without any refund to Customer.

2.24. **Reporting** – All written reports, with regards to any of Company services are provided by Company as is. Any additional changes if acceptable by Company may require additional support being purchased.

2.25. **Notification of Dissatisfaction** – Customer is encouraged to inform Company of any dissatisfaction or mishandling of support issues by contacting management_esc@mazebolt.com if the support and escalation channels failed to resolve Customer's issue to Customer's satisfaction.

2.26. **Consulting** – Consulting is not Professional Services, Support or Account Management. Consulting is performed at Company premises and not on-site at Customer. During the course of Consulting, Company may divulge opinions on 3rd party vendors, architectural setup or other technical or procedural setups which are not covered under Support or Account management. All such information is based on Company's expertise and experience and is divulged as is without Warranty or additional support.

2.27. **Measurement of Consulting hours** – The time invested by Company in the rendering of Consulting Services shall be measured in no less than half an hour (30 minutes) increments.