

Service Schedule D – FirstLight DDoS Protection & Mitigation Service

In addition to any other terms and conditions of Customer's Agreement with FirstLight, these Product Terms shall apply when Customer purchases FirstLight DDoS Protection & Mitigation Services.

1. Firstlight DDoS Protection & Mitigation Service.

- A. The FirstLight DDoS Protection & Mitigation Service uses an application and hardware platform designed to mitigate DDoS attacks at the Customer IP address, and subnet levels. The DDoS Protection & Mitigation Service consists of the following two functions:
 - (i) Always-on monitoring based on designated profiles
 - (ii) As-needed mitigation of malicious attacks upon FirstLight's automated system detection.
- B. To complete provisioning of the DDoS Protection & Mitigation Service, Customer shall designate the IP addresses Customer wants monitored. Each subscription of FirstLight DDoS Protection & Mitigation Service includes a profile that defines the list of protected IP addresses, protocols, and mitigation countermeasures associated with a supported hosted system. Profiles are customized to specific filters based on Customer baseline traffic. The profile is limited to a single host system and a maximum of 1000 IP entries (IP addresses or IP ranges in CIDR notation) per profile. Customer acknowledges that FirstLight DDoS Protection & Mitigation Service cannot perform unless and until Customer provides its profile(s) to FirstLight.
- C. When an attack is detected, the system shall auto-mitigate based on the rules in the applicable profile. The traffic to the protected IP addresses shall be redirected through FirstLight's mitigation systems with countermeasures applied in an attempt to limit the impact on legitimate traffic. When an attack subsides, as-needed mitigation shall end, and always-on monitoring shall continue.

2. Changes To Ip Addresses. Customer shall notify FirstLight if Customer wishes to modify the IP addresses that are being protected by the FirstLight DDoS Protection & Mitigation Service.

3. Insufficient Mitigation & Traffic Blocking.

- A. **Notification.** Due to the complexity and sophistication of DDoS attacks, Customer shall notify FirstLight if Customer believes the FirstLight DDoS Protection & Mitigation Service is not satisfactorily mitigating the attack consistent with industry practice for mitigation services. FirstLight shall confer with Customer regarding adjustments to the profile that may be available.
- B. **Mitigation Capacity.** FirstLight does not set per-customer limits on mitigation capacity. The limits to FirstLight's mitigation capacity depend on the type and nature of attacks and varying limitations across overall network capacity, data center network architecture and the configuration of the hosted system.
- C. **Traffic Blocking.** In the event that an attack impedes FirstLight's ability to operate the FirstLight network or negatively impacts other FirstLight customers, FirstLight may disregard packets, engage in upstream blocking, suspend access to the hosted system, or take other measures as necessary to protect FirstLight's network and other customers (collectively "Traffic Blocking") without prior notice. If Traffic Blocking is imminent or if FirstLight has already engaged in Traffic Blocking, FirstLight shall notify Customer promptly and work with Customer regarding the measures available, if any, to re-establish attack mitigation and connectivity to the hosted system.

4. Latency & Optimization. During an attack, and following one, Customer should expect increased latency across all affected IP addresses. No Network SLA or other credit is available due to latency experienced during an attack, even if the FirstLight DDoS Protection & Mitigation Service is active.

5. Firstlight DDoS Mitigation Subscription Service.

- A. **Exclusive Add-on Subscription.** The FirstLight DDoS Protection & Mitigation Service will only be installed with FirstLight-provided Internet as an add-on service. Customer acknowledges that FirstLight bears no responsibility for the performance of third-party provided Internet services and/or quality of data transmitted which are not owned, operated, or controlled by FirstLight.
- B. **Mitigation SLA.** FirstLight's auto-mitigation is guaranteed to detect and mitigate an attack within five minutes. If FirstLight fails to meet this guarantee, Customer is entitled to a credit of 10% of Customer's then current monthly fee for the FirstLight DDoS Protection & Mitigation Service for every five minutes during which FirstLight fails to activate the protection functionality of the FirstLight DDoS Protection & Mitigation Service (after the initial five minutes as applicable). The maximum total credit for any calendar month for failure to meet this guarantee shall not exceed 100% of Customer's then current monthly recurring fee for the FirstLight DDoS Protection & Mitigation Service. Credits that would be available for this limitation shall not be carried forward to future months nor be a set off for other FirstLight provided services.
- C. **Disclaimer.** Customer acknowledges that the FirstLight DDoS Protection & Mitigation Service may not successfully mitigate all attacks and may also result in some legitimate traffic being filtered from Customer's IP Address(es). FirstLight may discontinue the FirstLight DDoS Protection & Mitigation Service at any time by giving reasonable advance notice if FirstLight determines, in FirstLight's sole discretion, that the IP Address(es) and/or domains for which Customer has requested the service pose an undue risk to FirstLight's network or other customers.
- D. **Portal Security.** The Customer administrators and users are responsible for the security of all user ID and password information. This agreement applies to all IDs and passwords associated with the web-based application software. By enrolling for and using the DDoS Protection & Mitigation Service, the Customer accepts sole responsibility for the security and confidentiality of all passwords. Accidental or unauthorized disclosure of passwords or user ID or inappropriate use may have serious consequences and FirstLight shall have no liability for failure to securely maintain this information. Additionally, the Customer remains responsible for the use of each of its accounts, whether used under any name or by any person, and for ensuring full compliance with this agreement by all users of the account. In the event of a breach of security through the Customer's account, Customer must immediately contact FirstLight to prevent any further suspected data loss and/or breach.