MICRON21 DDoS SERVICES TERMS AND CONDITIONS

1. PURPOSE AND SCOPE

1.1 This clause governs all aspects of Distributed Denial of Service (DDoS) protection and mitigation for Services provided by Micron21, including scenarios where: (a) The Client has purchased and enabled DDoS Protection Services; or (b) The Client has expressly declined or not enabled DDoS Protection Services.

1.2 The DDoS Protection Service is not available with all Services and is made available at the absolute discretion of Micron21.

1.3 The Micron21 Shield service is not included by default and must be explicitly enabled or subscribed to as part of the Service Order.

2. DEFINITIONS

2.1 **Abnormal Traffic** - Sustained traffic exceeding the thresholds defined in Section 4.

2.2 **Client Services** - All equipment, virtual machines, IP addresses, and other resources assigned to the Client and hosted within Micron21 facilities.

2.3 **Commitment Bandwidth** - The data rate (in Mbit/s) purchased by the Client for IP-transit billing. If no commitment exists, it is deemed to be 100 Mbit/s.

2.4 **DDoS Protection Service** - The Micron21 DDoS Soak and Scrub service or Shield service as specified in the Service Order.

2.5 **Domestic Traffic** - Traffic whose source and destination are both within Australia.

2.6 **International Traffic** - Traffic whose source or destination is outside Australia.

3. CLIENTS WITHOUT DDoS PROTECTION

3.1 Applicability

These provisions apply to any Client who: (a) Expressly declines Micron21 DDoS Protection; (b) Has not added DDoS Protection to the services listed in the applicable Service Order; or (c) Has not enabled Shield service.

3.2 Traffic-Based Mitigation Thresholds

(a) If International Traffic to any Client IP group reaches or exceeds 20% of Commitment Bandwidth over a 60-second window, it will be classified as Abnormal Traffic.

(b) If Domestic Traffic reaches or exceeds 80% of Commitment Bandwidth over a 60-second window, it will be classified as Abnormal Traffic.

(c) For Clients without a bandwidth commitment, thresholds are fixed at:

- 20 Mbit/s (International)
- 80 Mbit/s (Domestic)

(d) For any transit service without DDoS protection, Micron21 reserves the right to null route traffic to all upstream peers globally for a minimum of 30 minutes if traffic is recorded at greater than twice the bandwidth commitment level towards any individual IP route for longer than 60 seconds.

3.3 Mitigation Actions

(a) Upon detection of Abnormal Traffic, Micron21 will automatically null-route, black-hole, or otherwise isolate all associated IP addresses to protect the integrity of its network and other client services.

(b) Isolation will remain in effect for at least one (1) hour, and continue until the Abnormal Traffic has ceased.

(c) During mitigation, Client Services will be unreachable from the Internet.

(d) Micron21 will not remove under any conditions a system generated null route once such action is taken.

3.4 Monitoring Limitations

(a) Micron21 only monitors aggregate bandwidth utilisation for Clients without DDoS protection. It does not monitor packets per second, session counts, or protocol-level detail.

(b) Traffic below the thresholds in Section 3.2 will pass unfiltered. The Client accepts that such traffic may overload downstream systems, and Micron21 bears no responsibility for such impacts.

3.5 Visibility and Notification

(a) Micron21 does not provide real-time alerts, telemetry, or detailed reports for mitigation actions under these terms for Clients without DDoS protection.

(b) Clients without protection will not receive automatic notification when isolation is triggered or resolved.

(c) An automatic system notification will be provided to the primary technical account contact only in the event the platform takes action.

3.6 Upgrade Restrictions

If an isolation event has occurred, the Client may request to activate DDoS protection; however, activation cannot take effect within the same calendar month in which the event occurred.

4. CLIENTS WITH DDoS PROTECTION

4.1 Service Provision

(a) Micron21 maintains and operates a DDoS Protection Service on the Micron21 Network for Clients who have ordered such service.

(b) The DDoS Protection Service provides protection against DDoS events that, in the sole opinion of Micron21, require mitigation using traffic scrubbing, filtering, black holing or any other action to protect the Micron21 Network and/or the Client's network.

(c) The Statement of Work will stipulate whether the Client has procured one or both of the following components:

- Micron21 DDoS Soak and Scrub
- Micron21 Shield Service

4.2 DDoS Soak and Scrub Service

(a) Comprises the provision of on-net DDoS protection to automatically mitigate DDoS events detected by the Micron21 DDoS detection system at all times.

(b) The Client may use BGP routing protocols or any other means to direct Client bound traffic to Micron21 DDoS mitigation devices for the duration of the attack only.

(c) The Client may contact the Micron21 support centre to request DDoS Soak and Scrub if an attack was not detected by Micron21 DDoS Detection platform.

(d) Provides layer 3 volumetric DDoS protection by default and, if purchased as an additional add-on, layer 4 session-based protection and layer 7 application protection.

4.3 Mitigation Methods

(a) Micron21 will in its sole discretion determine the method of mitigation to be used against a DDoS attack including, but not limited to, scrubbing, filtering and black holing of traffic.

(b) Scrubbing of DDoS traffic is limited to the current capacity of the on-net scrubbing system within the Micron21 Network.

(c) Where a DDoS attack is larger than the scrubbing capacity of the Micron21 mitigation system, Micron21 may black hole traffic or use other methods at its disposal to mitigate the attack.

(d) For DDoS protected services, traffic exceeding twice the committed bandwidth allocation to a single IP address will trigger a diversion for traffic to be inspected via the scrubbing platform, allowing traffic to pass if deemed legitimate.

4.4 Service Limitations

(a) DDoS protection is not available if in the sole opinion of Micron21: the traffic is not categorised as DDoS traffic, or the work required to identify, profile and mitigate the traffic is substantial, in which case Micron21 may charge a fee for service as agreed by the Client.

(b) Each order for a DDoS Protection Service may be applied only to one Service (a single connection or an aggregated billing group of internet connections) provided by Micron21 under a Service Order.

(c) All IP addresses associated with that Service will be monitored. Additional charges apply if the Client requires monitoring of additional IP addresses or a subset of a larger range of IP addresses already being monitored.

5. SHARED NETWORK FAIR USE POLICY

5.1 For Clients on shared network infrastructure, Micron21 enforces a fair use policy to ensure balanced network performance.

5.2 No more than 10% of total traffic may originate from a single source IP address at any time.

5.3 This rule ensures balanced inbound and outbound network load across all points of entry.

5.4 Micron21 reserves the right to rate-limit or restrict traffic from any IP that exceeds this threshold without notice.

5.5 Clients needing higher throughput from a single IP should use dedicated transit with custom traffic handling policies.

5.6 No single IP address can use more than twice the total committed bandwidth allocation before triggering a network event.

6. RECOMMENDATIONS AND CLIENT RESPONSIBILITIES

6.1 Micron21 recommends all transit Clients without DDoS protection to rate limit individual IP routes to not exceed more than the committed bandwidth to prevent legitimate traffic being null routed and/or increase bandwidth commitment to accommodate requirements.

6.2 The Client acknowledges that opting out of DDoS protection increases the risk of service disruption and assumes full responsibility for all resulting consequences.

7. LIABILITY AND INDEMNITY

7.1 **For Clients without DDoS Protection:** (a) Micron21 is not liable for any direct, indirect, or consequential damages, including loss of data, business interruption, or lost revenue, due to mitigation action. (b) Micron21 accepts no responsibility for globally null routing traffic if traffic levels towards an individual advertised IP address exceeded twice the committed bandwidth level. (c) Micron21 will not provide any logs, support, or investigation for any traffic issues in relation to any individual IP route which records greater than twice the bandwidth commitment level.

7.2 **For Clients with DDoS Protection:** With respect to the Micron21 DDoS Soak and Scrub service, Micron21 is not liable and otherwise excludes all liability in negligence or otherwise (whether under this agreement, any other Micron21 agreement or under any Micron21 SLA) in connection with, or in relation to: (a) Any traffic being rerouted away from the Client or any delays or other changes to traffic caused by routing, filtering or cleaning of the Client's traffic; (b) DDoS events not detected or protected by Micron21; or (c) Any traffic to, or from the Client's Service that may be delayed, dropped or otherwise affected.

7.3 The Client shall indemnify and hold harmless Micron21 from any third-party claims arising from mitigation events affecting Client Services.

8. ACCEPTANCE

By selecting DDoS Protection or No DDoS Protection in a Service Order, or continuing to use Micron21 services with or without an active Shield or DDoS protection subscription, the Client acknowledges and accepts these Terms and Conditions in full.