ARMOR DEFENSE
SERVICE LEVEL AGREEMENT

This Service Level Agreement ("SLA") outlines Armor's commitments ("Service Commitment") for (i) the end-to-end uptime for the Armor Complete Services ("Complete Services") and (ii) critical security incident notifications for both the Armor Anywhere Services ("Anywhere Services") and Complete Services, and sets forth the respective remedies available if Armor fails to meet these Service Commitments. This SLA and the credits provided for below ("Service Credits") are Armor's only obligation and customer's only remedy for Armor's failure to meet Service Commitments. Capitalized terms not defined herein will have the same meaning as in the applicable regional Terms of Services Agreement between customer and Armor (the "Agreement").

The Service Commitments under this SLA are:

1. **SECURITY INCIDENT NOTIFICATION GUARANTEE**

A. This guarantee is only applicable to customers who utilize either the Complete Services or Anywhere Services (collectively, the "Services").

B. Armor guarantees that customers will be notified of a Critical Security Incident within fifteen (15) minutes of Armor's knowledge of a security incident ("Critical Incident Notification Time" or "CINT"). "CINT" is defined as the time period between Armor identifying a Critical Security Incident and the time stamp associated with Armor's initial notification to the customer of the Critical Security Incident.

C. A "Critical Security Incident" occurs when Armor has positively identified a security incident within the scope of the Services that may have a significant impact to the environment protected by Armor. Examples of Critical Security Incidents include, but are not limited to:

• Successful brute force logins
• Detection of threat escalation of root privileges or lateral movement
• Post compromise activity such as outbound remote shell commands, attack tool downloads

Armor will initially notify the customer of a Critical Security Incident via a ticket in the Armor Management Portal. If Armor receives no response, it will use its best efforts to notify customer's primary point of contact by telephone. Customer is responsible for ensuring that its contact information is up to date in the Armor Management Portal.

D. **CINT Credits**

If Armor does not meet the CINT, the customer will receive a credit equal to five percent (5%) of the applicable monthly service Fees for the applicable Services for the impacted

account(s). Armor will apply the CINT Credits only against future payments otherwise payable by the customer for the applicable Services. The total cumulative CINT Credits claimed by the customer in any given month shall not exceed the amount owed by the customer for the applicable Services during that month.

E. **CINT Credit Claims**

(I) All CINT Credit claims should be communicated via a ticket in the Armor Management Portal within seven (7) calendar days of the incident giving rise to the claim. The ticket must include all relevant information, including, but not limited to the impacted server(s), the date, time and full description of the incident and any logs (if applicable). The customer's failure to provide the request and other information as required above will disqualify the customer from receiving a CINT Credit.

(II) To be eligible to make a CINT Credit claim, customer must use its best efforts to maintain a secure environment with hardened and patched applications and configurations, and to follow best security practices as recommended by Armor. Customer is expected to be responsive to the Armor Management Portal and phone notifications, and to take immediate action as required to bring a Critical Security incident to closure.

(III) To qualify for CINT Credit(s), customer (i) must be a Complete Services or Anywhere Services customer, (ii) cannot be ninety (90) or more days past due on payment to Armor, and (iii) must be in compliance with the Agreement for the Services and with Armor's Acceptable Use Policy.

2. '**END-TO-END' INFRASTRUCTURE UPTIME GUARANTEE**

A. This guarantee is only applicable to customers who utilize the Complete Services.

B. Armor guarantees an end-to-end uptime availability of 99.99% for the Complete Services. The "layers" and services needed to ensure the uptime of the Complete Services are:

• Physical Infrastructure (all power and HVAC infrastructure, including UPS, PDU and cabling)
• Armor Infrastructure (the Armor Network, firewalls, virtual firewall platform and infrastructure log collection devices)
• Storage Platform (includes all LUN(s), SAN Fabric, SAN Switches, and SAN Data drive availability)
• Compute Platform (includes all physical hosts and virtualization software)

Operations within the Complete Services (e.g., operating system and customer provided software) or within other services offered by Armor are excluded from this guarantee. For purposes of this SLA, the "Armor Network" is defined as the provision of access by

Armor to the Armor internal boundary to the Internet, as well as the internal network serving the front-end secure cloud hosting environment.

C. The following are excluded from this guarantee:

• The backend Armor-only management network;
• Routing anomalies, asymmetries, inconsistencies and failures of the Internet outside of Armor's control;
• Maintenance events as defined in Section F below;
• Customer instructed or requested actions, whether performed by the customer, Armor, or a third party, that impacts the availability of the Services.

Armor proactively monitors infrastructure uptime. The results of these monitoring systems are the exclusive determination of Complete Services uptime. Not more than once a month and upon request via the Armor Management Portal, Armor will provide customer with these results.

D. **Service Credits**

If Armor does not meet the "End to End Infrastructure Uptime Guarantee" (excluding Scheduled and Emergency maintenance as defined below), Armor will provide the following Service Credits:

Length of Downtime	Payment of Applicable Monthly Service Fees Impacted Services
>5 minutes – 45 minutes	10%
>45 minutes – 7 hours	20%
>7 hours	50%

(I) The payment of Service Credits will be based solely on the Fees for the Complete Services for the month in which the claim arises and only for the impacted account(s) for the Complete Services. Armor will only apply the Service Credits against future Complete Services payments otherwise payable by the customer. The payment for any single failure shall not exceed fifty percent (50%) of the monthly service Fees for the impacted components of the Complete Services. The total cumulative Service Credits claimed by the customer in any given month shall not exceed the amount owed by the customer for the Complete Services during that month.

(II) No Service Credits will be given for service interruptions: (i) caused by the action or failure to act by customer, customer's personnel, or any of customer's Users, (ii) due to

failure of any equipment or software provided by customer, (iii) which are the result of Scheduled or Emergency Maintenance, (iv) due to a force majeure event, (v) for which customer is entitled to a Service Credit for the same or contemporaneous Service Commitment failure, (vi) for downtime or other problems that may result from customer's use of the Beta Services, as defined in customer's Agreement with Armor, (vii) to the extent Armor offers customer a Self-Service Option and that results from customer's use of a Self-Service Option, or (viii) that occurs while customer is subject to any suspension action taken by Armor pursuant to customer's Agreement with Armor.

E. **Service Credit Claims**

(I) All Service Credit claims should be communicated via a ticket in the Armor Management Portal within seven (7) calendar days of the incident giving rise to the claim. The ticket must include all relevant information, including but not limited to the impacted server(s), the date, time and full description of the incident and any logs (if applicable).

(IV) To be eligible to make a Service Credit claim, customer must use its best efforts to maintain a secure environment with hardened and patched applications and configurations, and to follow best security practices as recommended by Armor. Customer is expected to be responsive to the Armor Management Portal and phone notifications, and to take immediate action as required.

(V) To qualify for Service Credit(s), customer (i) must be a Complete Services customer, (ii) cannot be ninety (90) or more days past due on payment to Armor, and (iii) must be in compliance with its Agreement for the Complete Services and Armor's Acceptable Use Policy.

F. **Maintenance Exceptions**

(I) **Scheduled Maintenance** Armor may from time to time conduct routine tests, maintenance, upgrades or repairs on any part of its networks, infrastructure, or the Services ("Scheduled Maintenance") and will use commercially reasonable efforts to provide prior notice (including at least fourteen (14) days' prior notice for customer-impacting maintenance). Armor will seek to perform scheduled maintenance outside of the business hours of the relevant data center (defined as Monday to Friday 09:00 to 18:00 of the time zone of the relevant datacenter).

(II) **Emergency Maintenance** In some instances, it may not be practical for Armor to give advance notice of maintenance, for example, in the event of an unforeseen disruption of service ("Emergency maintenance"). In these cases, Armor has the right to disrupt Services without prior notice.