SCC Annex II – Zeta Global – Technical, Physical, and Organizational Measures

A. Technical Measures

1. Information Security Policy

1.1. Zeta Global maintains a written information security policy which shall include, at a minimum, the approach adopted by Zeta Global to address the confidentiality, integrity, and availability of Zeta Global, its affiliates' and representatives', and its customers' confidential information, as applicable, which at least meets the minimum standards of (a) International Standard ISO.IEC 27001 and 27002 or (b) a similar industry-standard framework.

2. Testing and Scanning Procedures

2.1. Penetration testing: Upon request, Zeta Global provides Client with an executive summary of the results of penetration testing.

2.2. Information security certification: Upon request, Zeta Global provides Client with a third-party information security certification such as ISO 27K and SOC 2 Type II from an industry-recognized third party as of such then-completed year.

2.3. Vulnerability scanning: Upon request, Zeta Global provides Client with executive summaries of external, internal, and web application vulnerability scanning. If Client identifies elevated risks present within provided information, Zeta Global will promptly remediate identified risks at Zeta Global's expense. Zeta Global adheres to OWASP coding principles for web application code and uses static or dynamic application vulnerability scanning or manual code review, when appropriate. Zeta Global ensures that vulnerability scans periodically are conducted on devices and software present in its internal and external network environments and web applications to identify and remediate or have remediated any vulnerabilities within a documented timeframe. Zeta Global will provide Client with summaries of such scans and results upon request.

2.4. Penetration tests: Zeta Global conducts annual penetration tests on all its externally facing critical systems and applications from an industry-recognized independent third party at Zeta Global's expense. Zeta Global conducts similar such tests after significant changes are made to its network. Such penetration tests shall:

(a) be based on industry-accepted penetration testing approaches (e.g. NIST SP800-115),

(b) include testing from inside and outside the network,

(c) include testing to validate segmentation, and

(d) include network-layer, operating system, and application layer testing such that, at a minimum, they test against vulnerabilities identified in industry standards (e.g. OWASP Guide, SANS CWE Top 25, CERT Secure Coding).

3. Backups

3.1. Zeta Global maintains secure, usable, and traceable data/information backups to ensure that backups can be used when necessary.

4. Internal Hardware Protection

4.1. Zeta Global ensures that all computing and storage devices on its network, including but not limited to, workstations, servers, and network devices have endpoint protection in place consistent with industry standards, such as anti-malware, email, and application scanning, or antivirus.

4.2. Zeta Global has a tiered network architecture, which includes preventive and detective devices and where highly sensitive non-public information is in a secured and segregated network.

4.3. Zeta Global ensures that the network devices, servers, and workstations where Client information is located are hardened and continuously subject to minimum security baselines.

4.4. Zeta Global maintains an inventory of authorized devices that can be connected to its network environment and ensures that such inventory is reconciled periodically.

4.5. Zeta Global maintains an inventory of authorized software required for its network devices, servers, and workstations present in its network environment and ensures that such inventory is reconciled periodically.

4.6. Zeta Global maintains a change management methodology that ensures only approved changes are released and deployed in the production environment.

4.7. Zeta Global conducts periodic reviews of its cloud computing use based on the cloud security alliance risks and controls structure and addresses any elevated risks identified in a timely manner.

5. Periodic Reviews and Updates

5.1. Zeta Global conducts periodic reviews of its cloud computing use based on the cloud security alliance risks and controls structure and addresses any elevated risks identified in a timely manner.

5.2. Zeta Global promptly applies the latest firmware/security patches and updates on devices and software present in its network environment, expediting the application of critical and high-risk security patches and updates.

6. Encryption

6.1. Zeta Global ensures that all communications being initiated by Zeta Global or handling sensitive data are encrypted using industry-standard secure protocols.

B. Physical Measures

7. Data Center Security Measures

Zeta Global ensures appropriate data center physical security and data center environmental controls. Zeta Global utilizes the following physical security measures:

7.1. a closed-circuit television monitoring system with redundant power sources that provides recognizable images and usable recordings of entrances, exits, loading docks, and other high-security areas, and which maintains all images for at least 30 days and incident images indefinitely; The media portion is kept in a secured area.

7.2. distribution logs and for all issued access devices (including keys), secured storage areas for unissued devices, and regular audits of each of the foregoing;

7.3. access control alarms that actively are monitored by appropriate personnel;

7.4. identification (relying on governmentally issued credentials) and logging of individuals accessing Zeta Global's facilities (including visitors), as well as restriction of access to Client's assets (including intangible assets) to individuals authorized by Client.

C. Organizational Measures

8. Internal Employee Procedures and Policies

8.1. Role-based access control: Zeta Global maintains an up-to-date role-based access control based on data classification and job roles of employees, using the principle of least privilege and granting access only on a need-to-know basis.

8.2. Segregation of duties: Zeta Global maintains a segregation of duties, such that individuals performing application development are different from individuals managing production environments. Zeta Global employs technical and procedural controls to prevent developers and system administrators from obtaining access to production information.

8.3. Background checks: Zeta Global only utilizes personnel, including employees, contractors, and subcontractors, after performing background checks on them.

8.4. Security awareness training: Zeta Global ensures that its employees, contractors, and subcontractors receive appropriate security awareness training on a periodic basis.

8.5. Client's Standard of Conduct: If non-escorted access or access to Client systems is required, Zeta Global causes its representatives to comply with Client's standard of conduct.

9. Incident Response Plan

9.1. Zeta Global maintains an incident response plan that ensures that Zeta Global is adequately prepared to handle an incident, is able to accurately identify a Security Event as an incident, is able to contain the impact of the incident, has procedures in place to remediate the incident, has the ability to successfully recover from an incident and performs a root cause analysis of the incident.

10. Security Event

10.1. "Security Event" shall mean an instance of Zeta Global learning or having reason to believe that Client's confidential information has been accessed by an unauthorized person or disclosed in a manner not permitted by Zeta Global's agreement with Client, or that an incursion in any systems, processes, hardware or software used to store, transmit or that otherwise affect Client's confidential information has occurred.

10.2. In a Security Event, Zeta Global will:

10.2.1. as soon as reasonably practicable and in no event more than seventy-two hours after becoming aware of such Security Event, provide details of the same to Client including (i) the date of the Security Event, (ii) details concerning the data compromised, (iii) the method of the Security Event, (iv) appropriate Zeta Global security personnel contacts and security personnel contacts of its

representatives, (v) the name of any person or entity assisting Zeta Global with the investigation of the suspected or actual Security Event, (vi) a list of all parties known to have gained unauthorized access to confidential information for the limited purpose of assessing Client's exposure and (vii) any other information which Client reasonably requests from Zeta Global or its representatives concerning such suspected or Security Event, including any forensics reports;

10.2.2. grant access to Client's representatives or another person or entity agreed to by Client and Zeta Global (with each acting in good faith in the selection of such other person or entity) to Zeta Global's systems and premises to allow such representatives or such other person or entity to perform an investigation (including the installation of any monitoring or diagnostic software) deemed necessary by Client to locate the source of such breach; and

10.2.3. immediately take appropriate steps to ensure that any actual data security breach does not continue.

10.3. Public Authorities: Zeta Global will not notify law enforcement or federal or state regulatory authorities of any Security Event or other matter related to Client's security requirements without prior notice to Client unless otherwise required by applicable law.

10.4. Press Releases: Zeta Global will not issue any press release or other public announcement concerning a Security Event without prior approval of Client.

10.5. Read-only logs: Zeta Global maintains usable read-only logs of critical systems and events on network devices, key security systems, and workstation and server operating systems, and ensures that any suspicious activity is monitored and investigated and appropriate actions are taken subsequent to its detection.

11. Data Classification

11.1. Classes: Zeta Global defines classes of data/information based on applicable legal requirements and sensitivity levels of the related data/information and treats such data/information according to that classification.

12. Collaboration with Client

12.1. Client's security requirements: If Client believes that Zeta Global's or any of its representatives' security procedures in connection with the services provided to Client do not comply with Client's security requirements, Zeta Global will cooperate with Client to ensure that security measures and procedures that comply with Client's security requirements are promptly implemented.

12.2. Notification: Zeta Global will promptly notify Client if Zeta Global learns or has reason to believe that it or any of its representatives are not in compliance with any of Client's security requirements, whether or not a Security Event has occurred.