Wiz Security Addendum

This Wiz Security Addendum is incorporated into and made a part of the Wiz Subscription Agreement or other written agreement between Wiz and Customer that references this document (the "**Agreement**") and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement.

Wiz has implemented a comprehensive security, compliance and privacy management program under which Wiz maintains industry standard physical, administrative, organizational and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Services and Customer Data, including the measures set forth herein (the "**Security Program**"). Wiz regularly tests and evaluates its Security Program and may review and update its Security Program as well as this Wiz Security Addendum from time to time including to take in account technological developments, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

1. **IaaS and hosting.**

    a. IaaS Provider. Wiz's Platform is hosted on AWS.

    b. Hosting location. Wiz offers hosting in several locations including in the US, the EU and the UK. Customer may select the region in which their Wiz tenant will be hosted prior to the tenant being created.

2. **Wiz's Audits & Certifications.**

    a. Certifications. Wiz shall be assessed by independent third-party auditors on at least an annual basis under the following audits and certifications ("**Third Party Certifications**"): SOC2 Type 2, SOC3, ISO 27001, ISO 27701, ISO 27017 and/or ISO 27018. Wiz shall make available to Customer such Third-Party Certifications upon Customer's written request. To the extent Wiz decides to discontinue a Third-Party Certification, Wiz will adopt or maintain an equivalent, industry-recognized framework or standard.

    b. PCI-DSS. To the extent Wiz processes cardholder data in the provision of Services, Wiz shall perform a Payment Card Industry Data Security Standard Attestation of Compliance ("**AOC**") for Service Providers on an annual basis and shall provide such AOC to Customer upon Customer's written request.

3. **Encryption.**

    a. Encryption of Customer Data. Customer Data shall be encrypted by Wiz in transit (TLS 1.2. or above) and at rest (AES 256).

    b. Key Management. Wiz utilizes AWS' Key Management System (KMS) to encrypt Customer Data. Keys are rotated periodically and are stored only in the KMS in the region of the Customer's Wiz tenant.

4. **Authentication, Authorization, and Credential Management.**

    a. User Authentication (Wiz Employees). Wiz enforces user authentication and authorization on Wiz systems via Single Sign-on ("**SSO**") and multifactor authentication ("**MFA**").

    b. User Authentication (Customer using Wiz). Wiz supports SAML 2.0 compliant SSO applications, allowing customers to manage authentication for their own Wiz tenant.

    c. Secure Storage of Credentials. Wiz uses managed authentication services (Okta for Wiz's employee environment; Amazon Cognito for Wiz's software platform) to handle authentication and associated credential management, including encryption in-motion and at-rest for passwords and other forms of credentials. Cloud-native Key Management Systems, such as AWS KMS, are used to store other forms of access tokens and secrets.

    d. Role-based Access Control (RBAC) for Wiz Employees. Access to Wiz information assets is restricted, and

is granted to Wiz employees and contractors in order to fulfill their duties on a need-to-use basis and following the least privilege principle. Wiz employees and contractors are not granted access to any information asset that is not required by their work at Wiz. Wiz has defined various user roles, according to the positions and activities in the company. Each Wiz employee and contractor is assigned one of these roles and receives access control privileges relevant to that role. Quarterly reviews for user access will be conducted and access will be immediately revoked for unrequired access.

e. Role-based Access Control for Customers using Wiz. Wiz provides customers with the ability to define roles for their own Wiz users that control the information they see and the actions they perform.

f. Access to Customer Data. Wiz personnel will not access Customer Data except (i) as reasonably necessary to provide the Wiz Services under the Agreement; (ii) with Customer's permission; or (ii) to comply with the law or a binding order of a governmental body.

g. Minimum password requirements. Wiz shall follow the guidance provided by NIST 800-63B Digital Identity Guidelines to enforce password security controls, including length, complexity, re-use, lock-out, and use of multi-factor authentication. Passwords must never be stored in plain-text nor transmitted over unencrypted channels.

h. Session lifespan. Single-sign on sessions expire after 8 hours of inactivity with a maximum duration of 12 hours.

5. **Workstation and Device Security**

a. Session Lock out. End-user devices are set to screen lock and require a password after 15 minutes of inactivity.

b. Workstation Security Controls. For access to Wiz systems, Wiz personnel must use Wiz-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint firewall, (iii) anti-malware and endpoint detection and response (EDR) tools, and (iv) vulnerability management tools in accordance with Section 9.1 (Vulnerability & Detection Management).

c. Anti-malware. Wiz maintains anti-malware controls to automatically detect and prevent malicious files, user activity, and network activity on Wiz workstations, within Wiz's e-mail, and within Wiz's corporate cloud storage solutions.

d. Workstation Management and Hardening. Wiz utilizes system management technologies to ensure that all endpoints are appropriately configured, hardened, and patched following Wiz's technical procedures and applicable industry standards such as CIS Benchmarks.

e. Data Loss Prevention. Wiz utilizes Data Loss Prevention (DLP) technologies to monitor and control sensitive information that is stored or accessed on systems. Wiz workstations are restricted from using removable storage devices and media.

6. **Cloud Infrastructure Security**

a. Separation of Environments. Wiz's cloud network is divided into three segregated network environments: The development network, the staging network, and the production network. Each of these environments is segregated from the others and has its own privilege allocation and access control. There is no shared network, communication, or co-operation between the networks. Customer Data is never stored or accessed in development environments.

b. Infrastructure as Code. Wiz's cloud production environments are configured, provisioned, and managed through Infrastructure as Code (IaC), and subject to the controls defined in Wiz's Software Development Lifecycle (SDLC).

c. Remote Access. Wiz enforces device, network, authentication, and resource-specific authorization controls to limit access to development and production environments. Wiz does not automatically confer privileged access to any workstations or devices based on location.

d. Network Security. Wiz utilizes cloud-native network security technologies, including network security groups, Web Application Firewalls, access gateways, application load balancers, and VPC configurations, to restrict ingress and egress traffic in cloud environments to the minimum sets of services and addresses required for business functionality.

e. Cloud Infrastructure Hardening. Wiz utilizes its own instance of the Platform ("Wiz for Wiz") in conjunction with cloud-native security services to ensure that cloud resources are configured and secured in accordance with Wiz's internal technical procedures and industry standards such as the CIS AWS benchmarks.

f. Anti-malware. Wiz utilizes Wiz for Wiz in conjunction with cloud-native security services to detect and respond to potentially malicious activity on its cloud-hosted workloads or networks.

7. **Monitoring & Logging.**

a. Logging. Wiz maintains security auditing and logging capabilities for the infrastructure, SaaS applications, and cloud services that support its corporate, development, and production environments in accordance with Wiz's Information Security Policies. The use and activity of Wiz information assets is logged and audited for suspicious activity. Wiz preserves security-related logs for a minimum of 12 months unless otherwise specified in its security policies and procedures.

b. Detection and Response Operations. Wiz uses Security Information Event Management (SIEM), Detection, and Alert Notification technologies to centralize and analyze logs, apply detection criteria, and escalate and route events to the appropriate security teams.

c. Customer Access to Logs. Customers have access to system and user activity logs for their respective Wiz tenant via the Platform, and can export these logs to their own log storage or SIEM platforms as described in the Documentation.

8. **Security in the development process.**

a. SDLC. Software development in Wiz is performed according to Wiz's Change Management & Software Development Life Cycle (SDLC) procedures.

b. Security Reviews. Wiz conducts security reviews for significant changes, such as major new product features or changes that impact Wiz's security posture, during the design and development process.

c. Peer Reviews. Code changes must undergo secondary review and approval before being promoted to production.

d. Security Testing within the SDLC. Wiz uses security technologies to automatically scan for vulnerabilities, exposed secrets, and code security risks as part of the CI/CD pipeline.

9. **Vulnerability Detection & Management.**

a. Vulnerability Detection & Management. Wiz shall maintain a continuous vulnerability management process across its corporate and production environments to ensure that vulnerabilities and other threats are quickly identified, prioritized, and remediated. This includes carrying out internal vulnerability tests daily and external vulnerability tests regularly (at least quarterly). Vulnerabilities shall be remediated according to Wiz's Vulnerability Management Policy which shall meet or exceed industry standards. Wiz uses the Common Vulnerability Scoring System (CVSS) v3.1 and National Vulnerability Database (NVD) ratings as guidelines for patch prioritization and scheduling.

b. Penetration Testing. Wiz shall engage one or more independent third parties to conduct penetration tests of

the Service at least annually and upon major changes to the Services. Wiz will provide summary results of penetration tests to Customer upon written request.

10. **Administrative & Organizational Controls.**

    a. Personnel Security. All prospective Wiz employees go through pre-employment reference and/or background checks, according to the local HR policies and applicable laws.

    b. Personnel Agreements. All Wiz employees and contractors are required to sign a contract which includes a confidentiality obligation and are provided with Wiz's security policies, including Wiz's Acceptable Use Policy, when their work commences. Any change in an employee's position in Wiz or change in his or her access privileges immediately affects the employee's access via the centralized access control system.

    c. Personnel Training. All Wiz employees are required to complete security and privacy awareness training during onboarding and on at least an annual basis.

    d. Vendor Risk Management. Wiz maintains a third-party vendor risk management program, which includes a compliance, security, and privacy review for every third-party used in the provision of the Services and/or with access to Customer Data. The results of the risk assessment are reviewed by the security, legal and privacy team to ensure the third party maintains security measures consistent with the measures hereunder.

11. **Physical & Environmental Controls.**

    a. Cloud Environment Data Centers. Wiz only utilizes leading cloud providers who shall be required to have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks.

    b. Wiz Corporate Offices. Wiz's employees and subcontractors in each of Wiz's offices are subject to Wiz's physical minimum-security requirements which include use of CCTV with a defined retention period in accordance with applicable laws, badge only access with regular access reviews and requirements for visitors to be logged and accompanied by Wiz authorized personnel.

12. **Security Incident Notification and Response.**

    a. Wiz shall maintain a formal documented Information Security Incident Management Program designed to provide an effective and consistent process for managing security incidents.

    b. Security Incident notification. In any event of a reasonably suspected or successful unauthorized access, use, disclosure, modification, or destruction of Customer Data ("**Security Incident**"), Wiz will notify Customer within 48 hours of becoming aware of the Security Incident and shall promptly take reasonable steps to contain, investigate, and mitigate such Security Incident. Wiz shall provide Customer with assistance and information as reasonably required by Customer in order to fulfil its legal obligations.

    c. Security Incident Reporting and Response. Security Incidents are reported to Wiz's Chief Information Security Officer (CISO). The CISO acts according to Wiz's Incident Response Plan in classifying, handling, documenting, and reporting any incident. Customer may request a copy of Wiz's Incident Response Plan.

13. **Backup, Business Continuity & Disaster Recovery**

    a. Business Continuity and Disaster Recovery Plan. Wiz maintains industry standard business continuity and disaster recovery procedures, as further described in Wiz's Enterprise Resilience Policy ("**BCDRP**"), and will implement these procedures to minimize the impact of events, whether related to technology or operational failures, that may affect Wiz's ability to provide the Services. Wiz shall provide Customer with its BCDRP policy and procedures upon Customer's written request. Wiz's RTO shall not exceed 24 hours.

    b. Testing of BCDRP. Wiz shall conduct testing of its BCDRP at least annually and shall make the results of such testing available to Customer upon written request.

c. Backups and Disaster Recovery. Wiz leverages multiple Amazon services to backup Customer Data on both daily and monthly schedules. Each Customer tenant is allocated a disaster recovery tenant in a geographically distinct area. Where possible, Wiz will use a disaster recovery region in the same jurisdiction as the main data center. Wiz also keeps full and incremental backups of critical corporate data and logs in geographically distinct datacenters.

14. **Customer Audit Rights.** Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Wiz shall make available to Customer (or Customer's independent, third-party auditor that is not reasonably objected to by Wiz and that is bound by confidentiality obligations, ("**Permitted Auditor**")) a copy of Wiz's Third Party Certifications. Any Third Party Certifications and/or documentation made available by Wiz to Customer in accordance with this Section shall be Wiz's Confidential Information and shall only be used by Customer to assess compliance with this Security Addendum, and shall not be used for any other purpose or disclosed to any third party without Wiz's prior written approval and upon Wiz's request, Customer shall return all such documentation in Customer's possession or control. To the greatest extent possible, Customer shall utilize Wiz's Third Party Certifications and other security documentation and policies made available to Customer on Wiz's Trust Center to assess Wiz's compliance with its obligations under this Security Addendum. Only to the extent that Customer is not able to do so, and in any event, no more than once per year (except if otherwise required by applicable law) and following at least 45 days' notice in writing from Customer, at Customer's cost and expense, Wiz shall allow for and contribute to remote audits conducted by Customer or a Permitted Auditor. The Parties shall agree on the scope, methodology, timing and conditions of such audits in advance. Customer shall use reasonable endeavors to ensure that the conduct of each audit does not disrupt Wiz's business. In no event shall Customer be permitted to access any information, including without limitation, data that belongs to Wiz's other customers or such other information that is not relevant to Wiz's compliance with this the DPA. Unless otherwise agreed by the Parties, Customer shall use reasonable efforts to carry out the audit of Wiz's compliance with this Security Addendum together with the audit of Wiz's compliance with the DPA.

15. **Shared Responsibility.** Without derogating from Wiz's obligations hereunder, Customer acknowledges that it is responsible for implementing, running and managing the Platform on a day-to-day basis. In addition, Customer acknowledges and agrees that it has obligations with respect to the security of the Customer Data and the Services. Customer's responsibility includes but is not limited to: (i) the security of cloud environments it owns, operates, and connects to Wiz, and for configuration of its instance(s) of the Wiz Platform; (ii) provisioning Permitted Users with access to Customer's instance of the Wiz Platform, including: (a) managing instance-level administrators and other user privileges; (b) deauthorizing Permitted Users who no longer need access; (c) provisioning and configuring service account or API access; (d) enabling integrations with customer-owned or third-party technologies; and (e) ensuring that all Permitted User's keep all Wiz credential's confidential; and (iii) updating any Wiz provided software upon Wiz's announcement of such updates. A detailed overview of the parties' respective obligations as they relate to Customer's use of the Services is set forth in Wiz's Shared Responsibility Model described at https://docs.wiz.io/wiz-docs/docs/shared-responsibility-model. Wiz may update the Shared Responsibility from time to time, provided that any such update will not materially degrade the Parties' rights and obligations thereunder. Wiz provides customers with audit logs that record customer user account and application activity occurring within their respective Wiz Platform instance(s), however, Customer is responsible for monitoring its own instance's audit logs for security or other purposes. Customer agrees to notify Wiz upon becoming aware of any reasonably suspected unauthorized access to the Platform.