Wiz Minimum Security and Data Protection Requirements

1. Purpose

This Security and Data Protection Appendix ("**Appendix**") outlines the minimum security and data protection requirements for Service Providers who perform services for Wiz Inc. and its Affiliates (collectively, "**Wiz**"). This Appendix has been designed to minimize Wiz's exposure to damages which may result from unauthorized access to or use of Wiz Information or Wiz Systems (each as defined below) and set forth detailed obligations of Service Provider with regard to the availability, authenticity, integrity and confidentiality of Wiz Information. This Appendix forms an integral part of the agreement under which Wiz purchases services from Service Provider (the "Agreement"). Capitalized terms used herein but not defined shall have the meanings ascribed to them in the Agreement.

2. Definitions

2.1. "**Personnel**" means employees, contractors, subcontractors, consultants and/or service providers.

2.2. "**Wiz Information**" means collectively, (a) all information and data that is provided by Wiz or Wiz's Personnel to Service Provider (including through the Services or accessed or processed by Service Provider on behalf of Wiz, including any Personal Data; (b) all information and data relating to Wiz (and its affiliates, subsidiaries, customers, partners, employees, suppliers) or otherwise acquired by Service Provider for Wiz or its affiliates, subsidiaries, customers, partners, employees, suppliers, as a result of the Agreement, the Services, or the Parties' performance under or in connection with the Agreement; (c) all Wiz Confidential Information (as defined in the Agreement) and (d) all modifications, derivatives and/or output of the data specified in (a), (b) and (c).

2.3 "**Wiz Systems**" means any software, computing device or network operated by or on behalf of Wiz.

3. Technology Governance, Risk, and Compliance

3.1 Service Provider shall manage and implement a formal security and privacy management program ("**Security Program**"). The Security Program must manage risk, Service Provider's Personnel, processes and technology. Such Security Program shall be designed to protect Wiz Information, Wiz Systems, technology, services and solutions and shall include detailed procedures which govern the receipt, transmission, Processing, storage, control, distribution, retrieval, access, presentation, and protection of Wiz Information. The Security Program shall be communicated to and apply to all of Service Provider's Personnel. Service Provider shall ensure that its Security Program (a) accounts for known and reasonably anticipated threats, (ii) provides ongoing monitoring for new threats; (iii) meets or exceeds security and data protection industry best practices and (iv) meets requirements of applicable laws and regulations in all aspects of the Services provided to Wiz.

3.2 Service Provider shall implement and maintain appropriate administrative, physical and technical safeguards that prevent any unauthorized use, access, Processing, destruction, loss, alteration, or disclosure of the Wiz Information which, at a minimum, include the measures set forth in this Appendix. Supplier shall notify Wiz in writing of any technical, operational, organizational, or other change to its Security Program that may materially affect Wiz or Wiz Information, no less than 30 days before implementing any such change. Notwithstanding the foregoing and/or anything to the contrary, Service Provider shall not materially degrade its Security Program and/or any security measures applying to Wiz Information during the term of its Agreement with Wiz.

3.3 Service Provider shall test and update, at least annually, its Security Program against the requirements hereunder to confirm that its Security Program satisfies the requirements hereunder and appropriately takes into account technological developments and evolving threats. Service Provider shall ensure that security risks are identified, assessed, documented and addressed and appropriate security controls are applied, based on the assessed risk. Upon Wiz's request, Service Provider shall provide Wiz with the results of such tests.

3.4 Service Provider must maintain a data privacy program with assigned responsibilities and protection of Personal Data in

accordance with applicable law, including, Data Protection Laws. The program must protect data subjects with regard to the Processing of Personal Data or the free movement of such data. This program requires managing Personal Data under Service Provider's control throughout its life cycle by preventing unauthorized access or disclosure of Personal Data and imposing strict requirements on those that may access, view and/or otherwise Process Personal Data.

3.5 To the extent required by applicable laws, privacy impact assessments must be conducted to evaluate the impact to the Processing of Personal Data. Where applicable, Service Provider must have procedures for obtaining consent from data subjects to collect Personal Data, giving data subjects the ability to access, correct, opt-out, delete, restrict, make portable, or object to the processing of Personal Data. Where required by applicable law, a privacy notice or information banner must be in place, whenever Personal Data is collected, transmitted, processed, or stored by Service Provider. Service Provider shall maintain clear procedures around collecting Personal Data as required by applicable law.

4. Personnel

4.1 Service Provider shall establish and maintain formal security policies for its Personnel, including conducting appropriate background screening (as permitted by applicable laws) of all Personnel that may have access to Wiz's facilities, Wiz's Systems or Wiz Information. Such background screening (as permitted by applicable laws) shall include at a minimum: Social Security validation, National Criminal Database, Sex Offender Registry, and National Security/Terrorist Watch List checks, employment history (with a minimum of seven years back), education verification. Where Service Provider's Services involve Wiz's financial activities of any type, then a financial credit check must also be conducted and cleared prior to accessing any Wiz Information, Wiz systems or financial instruments to the extent permitted under applicable law.

4.2 Service Provider shall and shall ensure that its Personnel comply with Wiz's Code of Conduct which available via https://legal.wiz.io/legal#vendor-code-of-conduct. Service Provider represents and warrants that all Service Provider Personnel have received formal security and privacy training and are aware of Service Provider's information security policies, code of business and ethics, and confidentiality obligations and the risks to Service Provider and its customers in the event they should fail to comply with such policies and agreements. Training of Service Provider Personnel must also include guidelines and processes for identifying and reporting suspected security weaknesses and/or incidents.

4.3 Service Provider will remain fully liable to Wiz for its Personnel's performance of such contractual obligations and for the other acts and omissions of its Personnel. Service Provider will only permit Personnel to process Wiz Information after Service Provider has taken reasonable steps to confirm that such Personnel are capable of maintaining appropriate security measures (including reviewing all relevant attestation reports, copies of which will be provided to Wiz upon request). At least annually and in the event of a Security Incident involving Personnel, Service Provider will assess such Personnel's compliance with its contractual obligations and provide Wiz with a reasonably detailed summary of the audit results upon request.

5. Inventory

Service Provider shall maintain an inventory of all software, computing devices and networks that Process Wiz Information or are otherwise used to provide the Services. Service Provider shall Process Wiz Information and provide the Services only with software, computing devices and networks that are included on such inventory and that are owned by or operated on behalf of Service Provider.

6. Security Controls.

Service Provider shall maintain, and shall ensure its Personnel maintain, at least the following **security** controls with respect to Wiz Information and Wiz Systems, consistent with the highest of industry standards:

6.1 Physical and Environmental Security. Service Provider shall ensure that it maintains at all times physical and environmental security processes and procedures for facilities with access to, or storage of, Wiz Information ("**Facilities**"). Physical access to Service Provider's Facilities must be restricted, with all access recertified on a regular schedule. Detective monitoring controls (e.g., CCTV) must be in place with a defined retention period in accordance with applicable laws. Service Provider's Facilities must maintain appropriate controls, such as badge access, fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water damage detection. Physical material, paper, electronic material shall be destroyed through a

secure destruction process, including drive and paper shredding and/or magnetic destruction of electronic media. Environmental control components must be monitored and periodically tested by Service Provider.

6.2 Access Controls. Access controls whether physical or remote shall limit access to Wiz Information and Wiz Systems to only Service Provider Personnel who have a legitimate need for such access to provide the Services. Service Provider's access controls shall maintain the security principles of “segregation of duties” and “least privilege” with respect to Wiz Information and will include a process by which user accounts may be created only with proper Service Provider approval and such access shall be recertified at least quarterly. Without limiting the generality of the foregoing, Service Provider shall logically segregate and where applicable physically segregate Wiz Information such that Wiz Information its separate from any other data held by Service Provider and is not accessible by any third parties accessing their own data.

6.3 Password Management. Password and authentication controls shall be established, managed and controlled for all accounts with access to Wiz Information or Wiz Systems, whether direct or indirect. Service Provider shall deploy controls to lock accounts after no more than five invalid login attempts. All passwords shall have the following attributes: (a) minimum length of 10 characters; (b)complexity must include at least three of the following four criteria (i) one uppercase letter, (ii) one lowercase letter, (iii) one number, and (iv) one special character; (c)passwords cannot be any of the five (5) previous passwords; (d) initial or temporary passwords must be changed after first use; and (e) default passwords must be changed upon deployment. Passwords must never be sent in clear text format. Social Security Numbers or other national identifiers must not be utilized as user IDs or passwords for logging into applications.

6.4 Authentication. Authentication credentials must be protected by encryption during transmission. Login attempts must be limited to no more than five (5) consecutive failed attempts with user account being locked out for at least five (5) minutes upon reaching such limit. Sessions must be automatically terminated or activate a password-protected screensaver when user sessions are inactive for fifteen (15) minutes. Remote administration access by Service Provider or Service Provider Personnel to Wiz Information or Wiz Systems shall use two (2) factor authentication. With respect to any SaaS or software licensed by Service Provider to Wiz, Service Provider shall support implementation and integration with Wiz's standard single sign-on solution for end user authorization (OKTA). The access rights of all Personnel shall be removed upon termination of their employment, contract or agreement with Service Provider, or adjusted upon change of role.

6.5 Secure Configuration. Operational procedures and controls to ensure software, computing devices, and networks are developed, configured, and maintained according to prescribed internal standards consistent with the highest of industry standards. Security configurations shall be based on the principles of least functionality/privileges and all such configuration must be reviewed periodically for compliance with the terms under this Appendix. Supplier must implement controls over its communication network to safeguard Wiz Information. Service Provider shall maintain and provide Wiz upon request, a network diagram, to include all devices, as well as a data flow diagram. All network devices must have internal clocks synchronized to reliable time sources. Malware protection mechanisms must exist to detect and/or prevent against malware and other threats. Malware protection mechanisms must be configured to perform real-time or scheduled scans of systems, and alert when malware is discovered. All devices and malware protection mechanisms must be kept up-to-date with latest anti-virus software and definitions. Network and host-based intrusion detection and intrusion prevention systems (IDS and IPS) must be deployed with generated events fed into centralized systems for analysis. Service Provider must have policies, procedures, and controls that ensure proper control of an electronic mail and/or instant messaging system that displays and/or contains Wiz Information. Preventive controls must block malicious messages and attachments as well as prevent auto- forwarding of emails. Access to non-corporate/personal email and instant messaging solutions must be restricted. Data loss prevention (DLP) technology, processes, and/or solutions must be deployed to protect against the exfiltration of Wiz Information.

6.6 Network Security and Monitoring. Network security controls, including the use of firewalls, layered DMZs, and updated intrusion detection and prevention systems, to help protect systems from intrusion and limit the scope or success of any attack or attempt at unauthorized access to Wiz Information, Wiz Systems and/or Service Provider's software, computing devices, or networks.

6.7 Log Management. Log management procedures and technologies to create and maintain a complete audit trail to enable effective forensic investigations, including logging access to Wiz Information or Wiz Systems and an auditable history of all access changes for the purpose of detecting anomalous behavior that may indicate malicious events/incidents. Logs must be retained for

a period of no more than one hundred and eighty (180) days.

6.8 Vulnerability Management. Vulnerability management procedures and technologies to identify, assess, mitigate, and protect against new and existing internal and external security vulnerabilities and threats, including viruses, bots, and other malicious code must be implemented by Service Provider. At Service Provider's expense, Service Provider shall conduct, or cause to be conducted, periodic penetration testing and vulnerability scanning with respect to software, computing devices and networks used to provide the Services or otherwise Processing Wiz Information. Such testing and scanning shall be conducted at least annually by a qualified independent third Party engaged by Service Provider. Upon request by Wiz, Service Provider shall provide to Wiz with the results of such penetration testing and vulnerability scanning. Service Provider will promptly remediate any vulnerabilities identified by penetration testing or vulnerability scanning and any other security vulnerabilities of which Service Provider becomes aware. In addition to the foregoing, following Wiz's request, Service Provider shall allow Wiz or its designee to perform penetration testing and/or vulnerability scanning of Service Provider's software, computing devices and networks. Any critical vulnerabilities identified through intelligence gathering, vulnerability scans, or penetration testing must be prioritized and remediated within a well-defined timeframe commensurate with the vulnerability risk.

6.9 Patch Management. Patch management procedures and controls to timely implement security patches and updates to software and firmware.

6.10 Encryption. Unless otherwise by the Parties in writing, Service Provider shall encrypt, and shall ensure its Personnel encrypt, Wiz Information at rest and in transit using methods and protocols, including when Wiz Information is: (1) transmitted across any network, including the Internet; (2) transmitted via email; (3) stored on archival media (i.e., backups); or (4) stored on file servers or in application databases. In addition to the encryption requirements set forth above, the use of file transfer solutions to transmit Wiz Information must meet the following requirements: (1) files delivered to file transfer servers must have the data payload encrypted using the highest of industry standard and security protocols during transmission and while at rest on such servers; (2) files shall be removed from file transfer servers after successful receipt; and (3) decryption of encrypted files shall occur on secure servers with restricted access located in a secure zone. Service Provider shall not store or transmit user credentials in clear text.Service Provider shall only allow access protocols that encrypt or securely transmit login credentials (e.g., tunneling through SSH or TLS). Service Provider shall ensure that l encryption of at least 256 bits is used to encrypt all Wiz Information in accordance with this Section and that encryption keys are reliably managed.

6.11 Portable Devices and Removable Media. Wiz Information shall not be stored on any removable media or other portable device (including laptops, smart phones, and tablets). Service Provider shall employ data exfiltration controls to protect against, prevent, and detect unauthorized transfer of Wiz Information to portable devices. In the event that Service Provider requires the use of Wiz Information on such devices (including the ability to access Wiz Information from such devices), Service Provider shall obtain prior written authorization from Wiz and shall comply with any additional Wiz requirement.

6.12 Data Used for Testing. Service Provider shall not use any Wiz Information for testing purposes and shall not be used outside of any production environment. This includes but is not limited to test, development and QA environments.

6.13 Data Management. Service Provider and its Personnel must maintain a data dictionary or equivalent data description artifact, including any required metadata which records the types of Wiz Information Processed by Service Provider and/or its Personnel as well as the reasons for such Processing. Service Provider and its Personnel must have controls in place to allow Wiz to validate that types of Wiz Information held by Service Provider or its Personnel. All Wiz Information must be stored and retained in a manner that: (a) includes the capability to access and retrieve the data as needed; (b) avoids loss due to media decay or technology obsolescence; (c) provides reasonable safeguards against ordinary hazards, man-made hazards, and disasters; (d) is in accordance with applicable laws, regulations, and contractual obligations and/or (e) protects the Wiz Information from unauthorized access/alteration. If Service Provider or its Personnel hosts Wiz Information on behalf of Wiz, Wiz and its Personnel shall maintain and validate with Wiz (at least annually) a complete and accurate inventory of Wiz Information with the following attributes: (i) Description; (ii) Retention/Destruction Requirements and (iii) Location. Wiz Information Processed by Service Provider and its Personnel must follow a defined, regularly-reviewed procedure that manages the data throughout its lifecycle. Service Provider and its Personnel shall Process Wiz Information so solely to provide Services to Wiz. Service Provider and its Personnel must be able to demonstrate data origination.

6.14 Secure Disposal. Service Provider shall maintain disposal procedures and controls to ensure secure disposal of Wiz Information, in all forms of media, including secure removal or overwriting of Wiz Information from any electronic media before the media are made available for re-use. Notwithstanding anything to the contrary, unless agreed otherwise by the Parties in writing, within thirty (30) days of termination of the Agreement, Service Provider shall destroy all Wiz Information in an irretrievable manner or if requested by Wiz return to Wiz all such Wiz Information held by Service Provider or its Personnel. Upon Wiz's request, Service Provider shall confirm in writing the destruction or return of Wiz Information in accordance with the foregoing.

7. Geographic Restrictions

Unless agreed otherwise by the Parties, Service Provider, its Personnel shall only Process Wiz Information from locations pre-approved by Wiz in writing.

8. Reviews, Testing and Assessments

Service Provider shall conduct, and shall ensure its Personnel conduct, on at least a semi-annual basis, access control reviews to ensure Service Provider's access controls are operating effectively (i.e., access to Wiz and Wiz Systems is limited to individuals who have a "need to know"). Service Provider shall promptly remediate any access control failures identified during an access control review by revoking any unnecessary access, conduct a root cause analysis to determine the cause of the control failure, and remediate the cause of the control failure.

9. Certifications

Service Provider shall maintain throughout the Term applicable annual certification programs including, at the minimum a SOC 2 Type 2 certification or other equivalent certification if agreed by Wiz in writing ("**Certification**"). Service Provider shall provide proof of such Certifications to Wiz for Wiz's approval upon Wiz's request. Service Provider shall require auditors to conduct an examination of its compliance with the applicable Certification at least annually and upon any material change in Service Provider's Services or Service Provider's business, technology, or security practices. Following Wiz's request, Service Provider shall promptly deliver to Wiz a copy of the reports of such examinations. Service Provider shall prepare and implement a corrective action plan to remediate any findings in such reports. Wiz shall have the right to provide a copy of such reports and related information to their external auditors advisors and customers (subject to confidentiality obligations no less restrictive than those herein) and to any applicable regulators, but where permitted will use reasonable efforts to seek confidential treatment of such reports in any submission to regulators.

10. Questionnaires.

Service Provider shall promptly respond to requests from Wiz to complete security, privacy, and compliance questionnaires. Service Provider represents and warrants that all responses provided are accurate and complete. Such responses shall be deemed incorporated by reference in the Agreement. Service Provider agrees to promptly notify Wiz of any material changes to its responses during the Term of the Agreement.

11. Audits

Wiz reserves the right to perform information security assurance audits on Service Provider. The audit may be on-site at Service Provider's facility, remotely, via questionnaire, or through a third party. Except in the event of a regulatory audit or following a Security Incident, Wiz will provide Service Provider with a minimum of 30 days' notice prior of any onsite audits and such audits shall be carried out during Service Provider's regular business hours. Service Provider will respond to all questionnaires and resulting recommendations within a reasonable time period requested by Wiz. Service Provider agrees to discuss any findings of such audits with Wiz, and to provide related evidence of capabilities, remediation, and compliance activities. To the extent such audit reveals any breach of the requirements of this Agreement by Service Provider or Wiz otherwise determines that Service Provider is in breach of its obligations hereunder, Wiz shall have the right to terminate the Agreement.

12. Incident Management

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

include a procedure for conducting digital forensics including data collection, data/evidence preservation for future analysis, reporting of findings, and closure of incidents.

12.2 Service Provider shall notify Wiz as soon as possible but no later than within 48 hours upon becoming aware of any: (a) unauthorized, unlawful, or accidental access to or acquisition, use, loss, alteration, disclosure, corruption, destruction, or unauthorized processing of Wiz Information; (b) breach or compromise of, intrusion into, interference with, or unauthorized access to Service Provider's networks, systems, databases, servers, or electronic or other media on which Wiz Information is Processed or from which Wiz Information may be accessed, including those of Service Provider's Personnel, that compromises or could reasonably be expected to compromise Wiz Information, or (c) other event that could reasonably be expected to compromise the privacy, confidentiality, integrity, or availability of Wiz Information (each of the foregoing, a "**Security Incident**"). Notice under this paragraph shall be provided to Wiz at legalnotices@wiz.io and security@wiz.io with sufficient details regarding the Security Incident. Service Provider shall take action immediately, at its own expense, to investigate the Security Incident and identify, prevent and mitigate the effect of any such Security Incident and shall keep Wiz updated in regular intervals. Service Provider shall fully cooperate with Wiz to provide all information and evidence required by Wiz including logs. Notwithstanding anything to the contrary in the Agreement and without prejudice to Wiz's other remedies, following a Security Incident, Wiz may, in its sole discretion, immediately terminate the Agreement upon written notice to Service Provider and Service Provider shall promptly refund Wiz any prepaid but unused fees for the remaining Term.

12.3 Except as required by applicable law, Service Provider will not inform any third party of a Security Incident affecting Wiz Information (including via public announcements, communications to law enforcement or regulatory agencies, or similar statements) without Wiz' prior written consent, provided that general announcements of security breaches (not referencing or identifying Wiz or Wiz Information in any way) shall not require any such consent. Where such disclosures are required by law, Service Provider shall, except where it is legally prohibited from doing so, provide Wiz with reasonable prior notice and draft copies of any proposed notification and allow Wiz to provide comments. Service Provider shall promptly provide Wiz will all necessary information for Wiz to meet its legal obligations including with respect to notifications.

12.4 Service Provider shall bear all costs associated with the response to and remediation of a Security Incident and shall reimburse Wiz for all reasonable costs and damages resulting from such Security Incident including investigation and forensic costs, reasonable attorneys fees, notification costs, costs of any remedial measures required to be provided by Wiz under applicable laws, such as credit monitoring services and any fines, penalties or third party claims against Wiz arising from a Security Incident.

12.5 Service Provider shall not be released from its obligations hereunder with respect to a Security Incident in Service Provider's Personnel's or any third party for which Service Provider has enabled access to Wiz Information systems, and, as between the Parties, shall remain fully responsible for such incident.

13. Fraud Detection

Service Provider shall maintain an appropriate fraud and threat detection, prevention and mitigation program, processes and procedures for monitoring and reporting actual and suspected instances of fraud, and specific notification and communication, internally and to Wiz, must be established.

14. Development

Service Provider shall develop software using a secure system development lifecycle program ("SDLC") which limits security, integrity and availability risks. Service Provider must validate that the OWASP top Ten are tested for along with known vulnerabilities by using static and dynamic application testing tools. These processes should be aligned with the highest of industry standard application development security requirements. In addition, the SDLC shall include a formal vulnerability & patch management, change management and problem management. The SDLC must include a process for documenting and remediating vulnerabilities, coding errors, and design flaws prior to production using a risk-based approach. Service Provider shall ensure that it maintains all of the necessary rights and licenses to all third party and open-source code or software.

15. Technology Asset Management

Service Provider shall have a sufficient technology asset registration policy and procedure, including unique identifiers for all assets, appropriate classification, asset ownership, and asset location, including all applicable licensing and meeting all legal, regulatory, contractual, or support requirements. Service Provider shall (a) record changes to asset records, (b) ensure sufficient back up of asset registers, (c) carry out annual integrity validation of the asset registers, (d) carry out asset ownership recertification, and (e) update asset register updates when asset records are altered, (f)regularly audits license of assets, (g) implements procedures addressing lost/stolen assets, and remediation of unauthorized assets. A technology asset lifecycle management program must be maintained that includes accurate lifecycle status of all assets, identification of assets not in compliance with the lifecycle management policy, and notification to asset owners of non-compliant assets. A technology asset provisioning and disposal program must maintained to include only procuring technology assets from appropriately sourced suppliers and disposing of/removing/deleting all technology assets in a secure manner when they reach end of life. Service Provider shall ensure assets are transported in a secure manner.

16. Backups

Service Provider shall meet industry best standard requirements for retention of data, which at a minimum shall comply with all applicable laws and regulations governing data retention. All Wiz Information and data provide by the Services must be provided by Service Provider and available for export upon Wiz's request during or at the end of the Agreement. Data backups must be made to prevent data loss during a temporary failure of the primary environment or during a long-term outage.

17. Business Continuity and Disaster Recovery

17.1 Service Provider must have formal, comprehensive business continuity and disaster recovery plans to enable timely, orderly, and sustainable recovery of business, support processes, operations and technology elements associated with the Services provided to Wiz in accordance with industry best practices ("BCDR Plans"). Service Providers' BCDR Plans shall have a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of no more than 48 hours for all processes utilized to support the Services or functions being performed by Service Provider. Service Provider's BCDR Plans must (i) identify key resources and address business interruptions of those resources supporting all Services, including those provided by Service Provider's Personnel; and (ii) have recovery strategies in place to adequately address the following disruption scenarios to meet the service levels (as defined in the Agreement): (a) loss of staff, (b) loss of site (c) loss of application (where applicable);(d) loss of Supplier's Personnel; and (iii) will be tested at least annually. Service Provider's BCDR Plans shall include a formal disaster recovery plan and technical capability to limit service interruption and recover from a destructive cyber event where both the primary (production) and secondary (disaster recovery) systems or data have been compromised or destroyed, including but not limited to how to redeploy an application and restore associated data following a loss (including from cloud service providers and Personnel) and employment of a backup policy in order to meet full application recoverability. Within 48 hours, the Service Provider shall notify Wiz of an incident impacting the availability or provision Services being performed by Service Provider and keep Wiz notified of all outcomes and remediations of such incident. Failure by the Supplier to reinstate the Services in accordance with the RTO requirements set forth above shall entitle Wiz to terminate the Agreement and any applicable Order for cause, without incurring any liability, obligation, or penalty, in addition to any other rights and remedies available under this Agreement or applicable law.

17.2 Prior to the effective date, Service Provider shall provide Wiz with a copy of its current BCDR Plans, revision history, and the most recent reports or summaries regarding past testing of the BCDR Plans. Service Provider's BCDR Plans must be updated, reviewed and approved at least annually or as material changes occur within Service Provider's operating environment. Upon request, but no more than annually, the Supplier shall provide Wiz with a copy of the BCDR Plans. Any future updates or revisions to the BCDR Plans will be no less protective than the BCDR Plans in effect as of the Effective Term Date. Following Service Provider's testing of the BCDR Plans any deficiencies and/or failures should be addressed in a timely manner. All testing of Service Provider's BCDR Plans shall: (i) be conducted in conditions comparable to production; and (ii) demonstrate recovery within the established RTO. Test failures must be retested, and upon request, the Service Provider shall provide Wiz with copies of all reports and summaries resulting from the most recent testing of the BCDR Plans.

18. AI Technology

To the extent that the Service Provider uses artificial intelligence, machine learning or other similar technologies ("**AI**") in the services provided by Service Provider to Wiz ("**AI Features**" and "**Services**", respectively), the following provisions shall apply:

18.1 Input/Output; Ownership. Wiz may provide or input content, including but not limited to information, text, data or other materials, into or for use with the AI Features ("**Input**") and receive output generated and returned by the AI Features ("**Output**", and together with Input, "**AI Content**"). Wiz shall own all AI Content; however, Wiz understands and acknowledges that the AI Features may produce similar responses to similar prompts by other Service Provider's customers using similar AI Features functionality, and therefore, that certain intellectual property rights may not be enforceable. For the purposes of this Agreement, the definition of "Wiz Information" shall include AI Content, including Input and Output.

18.2 Use of Data. The Service Provider will only use Wiz Information, including the AI Content, as necessary to provide the AI Features and will not use Wiz Information, including the AI Content, to train or improve the AI Features or underlying AI models, without Wiz's prior written consent.

18.3 Third-Party Providers. The Service Provider will solely engage with third-party providers who contractually commit to using Wiz Information, including the AI Content, solely to provide the AI Features and not to train or improve their AI models, without Wiz's prior written consent.

18.4 Custom Model Training. To the extent the Service Provider allows Wiz to train Wiz's private instance of an AI model as part of the AI Features, Wiz Information used to train such private instance model will not be combined with other customers' data, will be solely used for the purposes of such private instance model and shall be destroyed upon termination of the Services.

18.5 Choice and Transparency. The Service Provider shall conspicuously disclose within the Services that the AI Features are powered by AI technology and shall identify the third parties that developed or licensed the underlying AI models. The AI Features shall only be enabled following explicit written consent from an authorized signatory of Wiz and Wiz shall have the option to opt out of the use of any AI Features at any time.

18.6 Responsible AI. The Service Provider is committed to responsible development and use of AI and follows responsible AI practices and standards and shall comply with all applicable laws in its provision of the AI Features to Wiz.

19. Insurance

Service Provider will maintain (during the Term and for 1 year thereafter) insurance cover which it would be customary to maintain having regard to its obligations under the Agreement, including but not limited to Commercial General Liability Insurance, Workers Compensation Insurance in accordance with statutory requirements, Crime insurance and Cyber & Professional Liability insurance. Upon request, Service Provider will provide to Wiz certificates of insurance evidencing such insurance. Service Provider agrees that the requirements under this clause in respect of insurance coverage will not limit its liability under the Agreement.

20. Termination

Any breach of this Appendix by Service Provider shall be deemed a material breach and Wiz may terminate the Agreement and/or any other agreements with Service Provider to the extent that Service Provider breaches the terms of this Appendix or immediately following a Security Incident.

21. Indemnification

Indemnification. Notwithstanding anything to the contrary in the Agreement or any agreement between the Parties, Service Provider shall indemnify, defend and hold harmless Wiz and each Wiz Affiliate against all losses, damages, or liabilities arising from any claim of any kind related to Wiz Information, or arising from or related to any breach of this Appendix and/or applicable law by Service Provider, Service Provider's Affiliates, or a subcontractor, or a Security Incident. Notwithstanding anything to the contrary in the Agreement or any agreement between the Parties, Service Provider's and Service Provider's Affiliate's liability related to Wiz Information, or for any breach of this Appendix, violation of applicable law and/or a Security Incident shall be unlimited.

22. Digital Operational Resilience Act (DORA)

Where Wiz deems Service Provider a subcontractor to Wiz under the Digital Operational Resilience Act (Regulation (EU) 2022/2554) (DORA), the obligations set forth in the DORA Addendum will apply in addition to the obligations set forth in this Appendix. The DORA Addendum is set forth here: https://legal.wiz.io/legal#vendor-DORA-requirements.