WIZ VENDOR SECURITY AND DATA PROTECTION MINIMUM REQUIREMENTS

1. Purpose. This Security and Data Protection Appendix ("**Appendix**") outlines the minimum security and data protection requirements for Vendors 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). This Appendix forms an integral part of the agreement under which Wiz purchased services from Vendor ("**Agreement**"). Capitalized terms used herein but not defined shall have the meanings ascribed to them in the Agreement.

2. Definitions.

2.1. "**Agreement**" means any relevant order, agreement, terms, and/or Purchase Order between the Parties.

2.2. "**Personnel**" means employees, contractors, subcontractors, consultants and/or vendors.

2.3. "**Wiz Information**" means collectively, (i) all information and data that is provided by Wiz or Wiz's Personnel to Vendor (including through the services or accessed or processed by Vendor on behalf of Wiz, including any Personal Data, as defined in the DPA; (ii) all information and data relating to Wiz (and its affiliates, subsidiaries, customers, partners, employees, officers, vendors) or otherwise acquired by Vendor for Wiz or its affiliates, subsidiaries, customers, partners, employees, officers, suppliers, as a result of the Agreement, the services, or the Parties' performance under or in connection with the Agreement; (iii) all Wiz Confidential Information (as defined in the Agreement) and (iv) all modifications, derivatives and/or output of the data specified in (i), (ii) and (iii).

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

2.5. "**Vendor Systems**" means any software, computing device or network operated by or on behalf of Vendor to Process Wiz Information or safeguard the security of Wiz Information.

3. Technology Governance, Risk, and Compliance.

3.1. Vendor shall manage and implement a formal security and privacy management program ("**Security Program**"). The Security Program must manage risk, Vendor'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 necessary portions of the Security Program shall be communicated to and apply to all of Vendor's Personnel on a need to know basis for the performance of their duties. Vendor shall ensure that its Security Program (a) accounts for known and reasonably anticipated threats, (b) provides ongoing monitoring for new threats; (c) meets or exceeds security and data protection industry best practices, and (d) meets requirements of applicable laws and regulations in all aspects of the services provided to Wiz.

3.2. Vendor 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. Vendor 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 thirty (30) days before implementing any such change. Notwithstanding the foregoing and/or anything to the contrary, Vendor 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. Vendor shall test and update, at least annually and, in any event, upon becoming aware of new technological risks or material changes affecting the Processing of Wiz Information or Vendor Systems, 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. Vendor 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, Vendor shall provide Wiz with the results of such tests.

3.4. If applicable, Vendor must maintain a data privacy program with assigned responsibilities and protection of Personal Data in accordance with applicable law, including, Data Protection Laws (as defined in the DPA). 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 Vendor'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, Vendor 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 Vendor. Vendor shall maintain clear procedures around collecting Personal Data as required by applicable law.

4. Personnel.

4.1. Vendor 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), and education verification. Where Vendor'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. Vendor shall and shall ensure that its Personnel comply with Wiz's Vendor Code of Conduct which is available via https://legal.wiz.io/legal#vendor-code-of-conduct Vendor represents and warrants that, prior to being granted access to Wiz Information, all Vendor Personnel have received formal security and privacy training on Vendor's obligations with respect to Wiz Information and the risks to Vendor and its customers in the event they should fail to comply with such policies and agreements. Training of Vendor Personnel must also include guidelines and processes for identifying and reporting suspected security weaknesses and/or incidents.

4.3. Vendor 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. Vendor will only permit Personnel to process Wiz Information after Vendor 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, Vendor 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. Vendor shall maintain an inventory of all software, computing devices and networks that Process Wiz Information or are otherwise used to provide or secure the services which shall be securely maintained, with access restricted to authorized Personnel strictly as required for their duties. The inventory shall include at a minimum (i) the date of its last update; (ii) infrastructure and hardware systems, communication components, and data security elements; (iii) software systems used for operation, maintenance, monitoring, and security of the services; (iv) software and interfaces for data exchange with the systems; and (v) a network diagram illustrating the connections between system components and their physical locations. Vendor 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 Vendor.

6. Security Controls.

Vendor 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. Vendor 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 Vendor'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 and shall monitor all entries and exits from the Facilities and, to the extent applicable, all setting and removing of equipment used to provide the Services. Vendor'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 Vendor.

6.2. Access Controls. Access controls whether physical or remote shall limit access to Wiz Information and Wiz Systems to only Vendor Personnel who have a legitimate need for such access to provide the services. Vendor'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 Vendor approval and such access shall be recertified at least quarterly. Without limiting the generality of the foregoing, Vendor shall logically segregate and where applicable physically segregate Wiz Information such that Wiz Information is separate from any other data held by Vendor and is not accessible by any third parties. Vendor's access to Wiz's environment shall be deactivated/disabled by Vendor after services have been completed. Any Vendor controlled IDs used to access, support, or maintain system components via remote access shall only be enabled during the time period needed and disabled by Vendor when no longer in use.

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. Vendor shall deploy controls to lock accounts after no more than five (5) invalid login attempts. All passwords shall have the following attributes: (i) minimum length of ten 10 characters; (ii) complexity must include at least three (3) of the following four criteria (1) one uppercase letter, (2) one lowercase letter, (3) one number, and (4) one special character; (iii)passwords cannot be any of the five (5) previous passwords; (iv) initial or temporary passwords must be changed after first use; and (v) 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 accounts 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 Vendor or Vendor Personnel to Wiz Information or Wiz Systems shall use two factor authentication including a physical authentication method under the individual's exclusive control (for clarity, this includes multi-factor authentication tools such as Google authenticator or equivalent or the use of Yubikeys). With respect to any SaaS or software licensed by Vendor to Wiz, Vendor 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 Vendor, 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. Vendor must implement controls over its communication network to safeguard Wiz Information. Vendor 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. Vendor 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 Vendor'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 detection, recording and forensic investigation of Security Incidents, including logging access to Wiz Information or Wiz Systems (including logging the user identity, date and time of access attempt, the system component attempted to be accessed and the type, scope and outcome of access attempts), and that detect and send alerts on any disabling or modification of normal operation, and prevent such actions to the extent possible. Vendor shall regularly review these logs and document identified issues and corrective actions taken. Such logs must be retained for a minimum period of twenty four (24) months.

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 Vendor. At Vendor's expense, Vendor 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 Vendor and Vendor shall discuss their findings, implement corrective measures, where required, and update its Security Program as necessary. Vendor shall retain records of such discussions and decisions for at least twenty four (24) months. Upon request by Wiz, Vendor shall provide to Wiz with the results of such penetration testing and vulnerability scanning. Vendor will promptly remediate any vulnerabilities identified by penetration testing or vulnerability scanning and any other security vulnerabilities of which Vendor becomes aware. In addition to the foregoing, following Wiz's request, Vendor shall allow Wiz or its designee to perform penetration testing and/or vulnerability scanning of Vendor'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. Vendor shall encrypt, and shall ensure its Personnel encrypt, Wiz Information at rest and in transit using methods and protocols, including when Wiz Information is: (i) transmitted across any network, including the Internet; (iii) transmitted via email; (iv) stored on archival media (i.e., backups); or (v) 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: (i) 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; (ii) files shall be removed from file transfer servers after successful receipt; and (iii) decryption of encrypted files shall occur on secure servers with restricted access located in a secure zone. Vendor shall not store or transmit user credentials in clear text. Vendor shall only allow access protocols that encrypt or securely transmit login credentials (e.g., tunneling through SSH or TLS). Vendor 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). Vendor shall employ data exfiltration controls to protect against, prevent, and detect

unauthorized transfer of Wiz Information to portable devices. In the event that Vendor requires the use of Wiz Information on such devices (including the ability to access Wiz Information from such devices), Vendor shall obtain prior written authorization from Wiz and shall comply with any additional Wiz requirement.

6.12. Data Used for Testing. Vendor 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. Vendor 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 Vendor and/or its Personnel as well as the reasons for such Processing. Vendor and its Personnel must have controls in place to allow Wiz to validate the types of Wiz Information held by Vendor or its Personnel. All Wiz Information must be stored and retained in a manner that: (i) includes the capability to access and retrieve the data as needed; (ii) avoids loss due to media decay or technology obsolescence; (iii) provides reasonable safeguards against ordinary hazards, man-made hazards, and disasters; (iv) is in accordance with applicable laws, regulations, and contractual obligations and/or (v) protects the Wiz Information from unauthorized access/alteration. If Vendor or its Personnel hosts Wiz Information on behalf of Wiz, Vendor 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 Vendor and its Personnel must follow a defined, regularly reviewed procedure that manages the data throughout its lifecycle. Vendor and its Personnel shall Process Wiz Information solely to provide services to Wiz. Vendor and its Personnel must be able to demonstrate data origination.

6.14. Secure Disposal. Vendor 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, Vendor shall destroy all Wiz Information in an irretrievable manner or if requested by Wiz return to Wiz all such Wiz Information held by Vendor or its Personnel. Upon Wiz's request, Vendor 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, Vendor and its Personnel shall only Process Wiz Information from locations pre-approved by Wiz in writing. Service Provider shall comply with Executive Order (E.O.) 14117 and shall immediately notify Wiz if Service Provider intends to engage in any type of transaction or data transfer that affect Wiz Information with entities located in or that have any connection with countries of concern (China including Hong Kong and Macau, Cuba, Iran, North Korea, Russia, and Venezuela) or covered persons, as defined by E.O. 14117.

8. Reviews, Testing and Assessments. Vendor shall conduct, and shall ensure its Personnel conduct, on at least a semi-annual basis, access control reviews to ensure Vendor's access controls are operating effectively (i.e., access to Wiz and Wiz Systems is limited to individuals who have a “need to know”). Vendor 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. Vendor shall maintain throughout the Term applicable annual certification programs including, at the minimum, a SOC 2 Type 2 certification and ISO/IEC 27001:2022(E) certification (“**Certification**”). Vendor shall provide proof of such Certifications to Wiz for Wiz’s approval upon Wiz’s request. Vendor shall require auditors to conduct an examination of its compliance with the applicable Certification at least annually and upon any material change in Vendor's services or Vendor's business, technology, or security practices and records of such examination must be kept by Vendor for at least twenty four (24) months. Following Wiz’s request, Vendor shall promptly deliver to Wiz a copy of the reports of such examinations. Vendor shall prepare and implement a corrective action plan to remediate any findings in such reports and assess whether any updates are required to its Security Program as a result. 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. Audits. Vendor shall provide to Wiz upon Wiz's request at least annually confirmation of its compliance with its obligations under this Appendix and information on the manner in which it implements such obligations. In addition, Wiz reserves the right to perform audits on Vendor which may be on-site at Vendor'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 Vendor with a minimum of thirty (30) days notice prior to any onsite audits and such audits shall be carried out during Vendor's regular business hours. Vendor will respond to all questionnaires and resulting recommendations within a reasonable time period requested by Wiz. Vendor 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 Vendor or Wiz otherwise determines that Vendor is in breach of its obligations hereunder, Wiz shall have the right to immediately terminate the Agreement and Vendor shall promptly refund Wiz any prepaid by unused fees for the remaining term.

11. Incident Management.

11.1. Vendor 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.

11.2. Vendor shall notify Wiz as soon as possible but no later than within forty-eight (48) hours upon becoming aware of any reasonably suspected: (i) unauthorized, unlawful, or accidental access to or acquisition, use, loss, alteration, disclosure, corruption, destruction, or unauthorized processing of Wiz Information; (ii) breach or compromise of, intrusion into, interference with, or unauthorized access to Vendor'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 Vendor's Personnel, that compromises or could reasonably be expected to compromise Wiz Information, or (iii) 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. Vendor 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. Vendor 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 Vendor and Vendor shall promptly refund Wiz any prepaid but unused fees for the remaining term.

11.3. Except as required by applicable law, Vendor 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, Vendor 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. Vendor shall promptly provide Wiz will all necessary information for Wiz to meet its legal obligations including with respect to notifications.

11.4. Vendor 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.

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

11.6. Vendor shall hold periodic discussions (at least quarterly) regarding any Security Incidents including any events raising concerns of unauthorized Processing of Personal Data, Processing beyond the scope of granted authorization, or a compromise of the integrity of Personal Data, and assess the need to update its Security Program accordingly. Vendor shall retain records of such discussions and decisions for at least twenty four (24) months.

12. Fraud Detection. Vendor 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.

13. Development. Vendor shall develop software using a secure system development lifecycle program ("**SDLC**") which limits security, integrity and availability risks. Vendor 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. Vendor shall ensure that it maintains all of the necessary rights and licenses to all third party and open-source code or software.

14. Technology Asset Management. Vendor 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. Vendor shall (i) record changes to asset records, (ii) ensure sufficient back up of asset registers, (iii) carry out annual integrity validation of the asset registers, (iv) carry out asset ownership recertification, and (v) update asset register updates when asset records are altered, (f)regularly audits license of assets, (vi) 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. Vendor shall ensure assets are transported in a secure manner.

15. Backups. Vendor 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 provided by the services must be provided by Vendor 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.

16. Business Continuity and Disaster Recovery

16.1. Vendor 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**"). Vendors' BCDR Plans shall have a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of no more than forty-eight (48) hours for all processes utilized to support the services or functions being performed by Vendor. Vendor's BCDR Plans must (i) identify key resources and address business interruptions of those resources supporting all services, including those provided by Vendor'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): (1) loss of staff, (2) loss of site (3) loss of application (where applicable) and (4) loss of Supplier's Personnel; and (iii) will be tested at least annually. Vendor'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 forty-eight (48) hours, the Vendor shall notify Wiz of an incident impacting the availability or provision services being performed by Vendor 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 Purchase 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 and Vendor shall promptly refund Wiz any prepaid by unused fees for the remaining term.

16.2. Prior to the effective date, Vendor 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. Vendor's BCDR Plans must be updated, reviewed and approved at least annually or as material changes occur within Vendor's operating environment. Upon request, but no more than annually, Vendor 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 applicable Purchase Order issue date. Following Vendor's testing of the BCDR Plans any deficiencies and/or failures should be addressed in a timely manner. All testing of Vendor'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 Vendor shall provide Wiz with copies of all reports and summaries resulting from the most recent testing of the BCDR Plans.

17. Deidentified Data. To the extent that Wiz provides Vendor with data that has been deidentified so that it cannot be associated with a specific individual ("**Deidentified Data**"), Vendor shall:

17.1 not attempt to reidentify, or permit or enable any third party to reidentify, any individual who is the subject of the Deidentified Data;

17.2 not combine the Deidentified Data with other information if doing so could reasonably be expected to reidentify an individual;

17.3 use the Deidentified Data solely for the purposes specified in the Agreement;

17.4 maintain all appropriate measures to prevent the reidentification of the Deidentified Data and to prevent unauthorized access or disclosure; and

17.5 impose these same obligations on any subcontractor who receives Deidentified Data from the Vendor.

18. AI Technology. To the extent that the Vendor uses artificial intelligence, machine learning or other similar technologies in the Services, Vendor shall comply with Wiz's Vendor Artificial Intelligence Terms set forth at https://wiz.pactsafe.io/legal#vendor-ai-terms.

19. Financial Services. Where Wiz deems Service Provider a subcontractor (or equivalent designation) to Wiz under the Digital Operational Resilience Act (Regulation (EU) 2022/2554) ("**DORA**"), Prudential Standard 230, or other financial services regulation, the obligations set forth in the Wiz Financial Services Addendum set forth here: https://legal.wiz.io/legal#vendor-finserv-requirements will apply in addition to the obligations set forth in these Wiz Vendor Security and Data Protection Minimum Requirements.

20. Termination. Any breach of this Appendix by Vendor shall be deemed a material breach and Wiz may terminate the Agreement and/or any other agreements with Vendor to the extent that Vendor breaches the terms of this Appendix or immediately following a Security Incident. If Wiz terminates for breach of this Appendix Vendor shall promptly refund Wiz any prepaid by unused fees for the remaining term.

21. Indemnification. Notwithstanding anything to the contrary in the Agreement or any agreement between the Parties, Vendor shall indemnify, defend and hold harmless Wiz and each Wiz affiliate against all losses, damages, or liabilities arising from any claim of any

kind arising from, or related to, any breach of this Appendix, applicable law or a Security Incident. Notwithstanding anything to the contrary in the Agreement or any agreement between the Parties, Vendor's liability related to Wiz Information, or for any breach of, or related to, this Appendix, violation of applicable law and/or a Security Incident shall be unlimited.