

WIZ INCIDENT RESPONSE SERVICES TERMS

These Wiz Incident Response Services Terms (“**IR Terms**”) supplement and form part of the Wiz Subscription Agreement or other agreement entered into for Wiz services (the “**Agreement**”) by and between Wiz and Customer (each as defined in the Agreement) and apply to Customer’s use of Wiz IR Services (as defined below). For the avoidance of doubt, the IR Services are part of the Wiz Services (or other similar term) described in the Agreement. Capitalized terms not defined in these Terms have the meanings given to them in the Agreement. In the event of any conflict between these IR Terms and the Agreement, these IR Terms will control with respect to the IR Services unless Customer and Wiz have separately entered into IR Terms which expressly states the Parties’ intent to amend the terms set forth herein, in which case Customer’s access to and use of the IR Services will be governed by such amended terms. Notwithstanding anything to the contrary, if the IR Services are identified as Preview Features within the Platform, the preview terms in the Agreement shall apply to such IR Services for as long as they remain Preview Features.

1. DEFINITIONS

1.1 “**Incident**” means any actual or suspected event that:

- (a) compromises the confidentiality, integrity, or availability of Customer’s computer systems or networks;
- (b) involves the unauthorized access, use, disclosure, modification, or destruction of Customer’s data; or
- (c) results from malicious or potentially malicious actions, including but not limited to malware, unauthorized code, or denial-of-service attack.

1.2 “**IR Services**” means Wiz’s consulting services for responding to an Incident, which may include scoping, investigation and forensic analysis, recommending containment and remediation measures, and providing an Incident report. The specific scope of services will be determined based on the nature and severity of the Incident, and agreed upon in advance with Customer.

2. IR SERVICES ACTIVATION

Upon receiving notice of or discovering an Incident, Customer may request Wiz to initiate IR Services through the Platform or in any other manner determined by Wiz (“**Activation Request**”). In the Activation Request, Customer shall be required to include a description of the current known scope of the Incident, a point of contact who is authorized by Customer to instruct and work with the Wiz IR Services team during the course of the IR Services and any other communication protocol instructions requested by Customer. Wiz will provide IR Services remotely unless both Parties agree otherwise in writing.

3. ACCESS TO CUSTOMER DATA; DEPLOYMENT OF ADDITIONAL WIZ SERVICES

3.1 **Access to Customer Data.** Wiz may request that Customer provides designated Wiz IR Services personnel with access to Customer’s Wiz tenant to review configuration hygiene, issues, findings, logs and any other information contained within the Customer’s Wiz tenant in connection with the investigation and IR Services. Wiz IR Services

personnel may also request any additional data or access as needed to provide the IR Services and Customer shall be solely responsible for facilitating such access and for collecting and providing the requested data to Wiz. Where data is requested, Customer shall provide such data to Wiz using a mutually agreed secure method. All such data shall be considered Customer Data as defined under the Agreement and shall be subject to the confidentiality and security obligations in the Agreement and, to the extent such data includes Customer Personal Data, to the DPA in place between the Parties. Wiz will not be responsible for any delays due to Customer's failure to comply with Wiz's requests or provide access or information requested by Wiz under this Agreement.

3.2 Deployment of Additional Wiz Services. Following an Incident, Wiz may provision additional Wiz Services on the Customer's Wiz tenant on a free of charge basis for a limited period that Wiz determines is required for the IR Services. Customer shall co-operate with Wiz in order to ensure effective deployment of such additional Wiz Services.

4. CUSTOMER OBLIGATIONS

Customer shall and agrees to:

4.1 Be responsible for the accuracy of the data it provides, and for implementation of security and access controls when providing Wiz personnel with access to such data.

4.2 Manage the collection and dissemination of all information regarding an Incident within Customer's organization and to external parties as required by Customer.

4.3 Be responsible for the decision to implement (or not to implement) Wiz recommendations, taking any actions required to do so, and the results achieved from such implementation.

4.4 Be responsible for and facilitate all communications between Wiz and any Customer's third-party service providers, to the extent required by Wiz to provide the IR Services.

4.5 Be responsible for making any determinations regarding legal or regulatory actions following an Incident, including notification to regulatory authorities or affected individuals.

4.6 Cooperate with Wiz's requests in its provision of IR Services in a timely manner.

4.7 Be responsible for revoking Wiz's access to Customer's Wiz tenant and other systems provided after completion of the IR Services.

5. DISCLAIMERS

WIZ DOES NOT WARRANT OR GUARANTEE: (A) IDENTIFICATION OF EVERY EXISTING INCIDENT OR ALL COMPROMISED SYSTEMS; (B) COMPLETE RESOLUTION OF AN INCIDENT; (C) ERROR-FREE INCIDENT CLASSIFICATION, (D) CORRECT INCIDENT PRIORITIZATION; (E) THAT IR SERVICES ARE SUCCESSFUL IN REMOVING OR RESOLVING INCIDENTS; (F) ANY SPECIFIC OR DESIRED OUTCOME OF IR SERVICES; (G) SATISFACTORY INCIDENT RESPONSE OR THREAT HUNTING; (H) DATA RECOVERY; OR (I) PREVENTION OF FUTURE INCIDENTS.

THE IR SERVICES ARE PROVIDED "AS IS" WITHOUT ANY OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY,

OR NON-INFRINGEMENT.

6. THREAT INTELLIGENCE

Any threat indicators, tactics, techniques, and procedures (TTPs), malware samples and other threat intelligence or threat actor data and potentially malicious artifacts discovered during IR Services are considered Account Data (as defined under the Agreement) and may be used by Wiz to improve Services in each case without derogating from Wiz's confidentiality, data and security obligations hereunder and without identifying Customer or Customer Data to other customers or third parties which are not deemed Authorized Recipients under the Agreement.

7. TERM AND SURVIVAL

7.1 These IR Terms continue while Customer is receiving IR Services.

7.2 Sections 4 (*Customer Obligations*), 5 (*Disclaimers*), 6 (*Threat Intelligence*), 7 (*Term and Survival*) and 8 (*Miscellaneous*) will survive termination or expiration of these IR Terms and the Agreement.

8. MISCELLANEOUS

Notwithstanding anything to the contrary in the Agreement, Wiz may update these IR Terms, and such updates will be made available at www.wiz.io/legal/legal-hub (or any successor page(s)). Except for any updates required to comply with applicable law, any updates to these IR Terms made after Customer's acceptance shall become effective for Customer upon the effective date of a new Order entered into by Customer. Notwithstanding the foregoing, any modifications made to these Terms whilst the IR Services are identified as Preview Features shall be effective immediately.