Huntress Labs Incorporated
6021 University Blvd, Suite 450
Ellicott City, MD 21043

Huntress Labs Incorporated

Security Addendum

Effective and Last Updated March 14, 2023

This Security Addendum is incorporated into and made a part of the Terms of Service between **Huntress Labs Incorporated** and its affiliates and subsidiaries and Customer (or if applicable, the superseding written agreement between Customer and Huntress) (the "**Agreement**"). Terms used on this page but not defined have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this Security Addendum, this Security Addendum shall govern.

Huntress maintains a comprehensive security program, under which Huntress implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Services and Customer Personal Data (the "**Security Program**"), including, but not limited to, as set forth below. Huntress regularly tests and evaluates its Security Program, and may review and update its Security Program as well as this Security Addendum, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

The Security Program includes, at a minimum, the following controls:

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of the Security Program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Huntress' organization, monitoring and maintaining compliance with the Huntress' policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include, at a minimum, logical segregation of data, restricted (*e.g.* role-based) access and monitoring, and utilization of commercially available industry standard encryption technologies for Personal Data that is transmitted over public networks (*i.e.,* the Internet) or when transmitted wirelessly or at rest or stored on portable or removable media (*i.e.*, laptop computers, CD/DVD, USB drives, back-up tapes).

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (*e.g.*, granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

5. Password controls designed to manage and control password strength and usage including prohibiting users from sharing passwords and requiring that the Huntress' passwords that are assigned to its employees: (i) be at least sixteen (16) characters in length, (ii) not be stored in

Huntress Labs Incorporated
6021 University Blvd, Suite 450
Ellicott City, MD 21043

readable format on the Huntress's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of data centers, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of the Huntress's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Huntress' possession.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to the Huntress' technology and information assets.

10. Incident management procedures designed to allow Huntress to investigate, respond to, mitigate and notify of events related to the Huntress' technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls, layered DMZ architectures, and traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters.