ADDITIONAL TERMS FOR PARTNER SERVICES

("ADDITIONAL TERMS")

These additional terms and conditions apply to Partners who choose, from time to time, to provide Partner Services.

1. **Partner Services**.

1.1 **Partner Services**. During the Term, and subject to the terms and conditions of this Agreement and the Partner Guide, Armis grants Partner, on a non-transferrable, non-sublicensable, non-exclusive basis, the right to provide to Customers limited-time professional services relating to the deployment, implementation, and initial configuration of the Armis Solutions within the Customer environment ("**Partner Services**"). Partner Services may include delivery and installation of Collectors and Collector Technology, onboarding, migration and configuration of the Armis Platform, process consulting, and End User training. Partner Services are generally one-time in nature but may occur periodically during a Customer's subscription in connection with deployments at new sites. Partner may use the Armis Solutions to provide the Partner Services, as well as Partner's own technology, products, services, and other assets owned or rightfully used by Partner outside of this Agreement, including any software, hardware, processes, or services used by Partner ("**Partner Assets**"). Partner Assets specifically excludes Armis Assets and Armis IP.

1.2 **Performance**. Partner shall perform Partner Services to the best of Partner's ability, in a timely and professional manner, in accordance with the Documentation, this Agreement, and the Partner Guide, and using competent personnel with the necessary skill and expertise. Partner Services may be provided only to Customers within the Territory and solely for Customers' internal business purposes. Partner shall perform Partner Services for its own account under an agreement between Partner and Customer that makes it clear Partner is the provider of the Partner Services and not Armis. Partner may provide the Partner Services through an Affiliate, and Partner is responsible and liable under the terms of this Agreement for such Affiliates. Partner shall not subcontract any part of the Partner Services to any third party that is not an Affiliate without Armis' prior written consent, which may be withheld or granted in Armis' sole discretion.

1.3 **Responsibility**. Partner is solely responsible for the performance and provision of Partner Services and for any action or inaction of Partner's End Users. Armis is not responsible for any losses or damages arising due to any breach of this Agreement (or the applicable Customer Agreement) by any End User of Partner or any other personnel, agent, or advisor of Partner, including unauthorized persons who manage to gain access to the instance of the Armis Platform through usernames, passwords, and accounts under Partner's control and management. Partner shall prevent unauthorized third parties from accessing the Armis Platform during any time Partner is providing Partner Services. Partner shall notify Armis immediately upon becoming aware of any unauthorized use of the Armis Platform.

1.4 **Fees**. Partner may determine whether and how to charge for Partner Services in its sole discretion, provided that Partner Services must be sold or provided to Customer under a separate SKU or line item that is distinct from any SKU or line item for Armis Solutions.

1.5 **Personnel**. Partner shall use its own personnel who are lawfully employed in the jurisdiction where Partner Services are being provided and who have successfully passed an industry standard criminal/employment/education background check. Partner shall retain background check information for such personnel for the duration Partner regularly retains such information and at Armis' request shall provide such information to Armis, which may be redacted or summarized to comply with applicable Laws and Armis' contractual obligations to Customers. Subject to applicable law, Partner shall not permit any person who has not successfully passed such background check to perform any Partner Services. Subject to applicable Laws, no Partner personnel who has been convicted of fraud, theft, or similar act of dishonesty is eligible to provide Partner Services. Partner shall comply with Customer's requirements with respect to the Partner Services, including any security rules, policies, or procedures governing access to Customer's premises.

1.6 **Security**. During the time Partner is providing Partner Services, Partner shall maintain commercially reasonable administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of the Partner Assets and/or systems used to provide Partner Services to Customers, including access to and processing of Customer's data, at levels substantially similar to or exceeding the Armis Partner Data Security Requirements (as may be updated by Armis from time to time upon reasonable written notice).

1.7 **Other Services**. This Agreement does not authorize Partner to perform, and Partner Services specifically excludes, custom onsite work or managed services, which are ongoing operation, use, maintenance, and support services provided on a continuous or periodic basis after the Armis Solution is deployed or implemented at a given site or for a given Customer. Armis may authorize Partner to provide such services only by executing a separate written agreement with Partner.

****

ARMIS PARTNER INFORMATION SECURITY REQUIREMENTS FOR PARTNERS PROVIDING PARTNER SERVICES OR SUBCONTRACTED SERVICES

The terms set forth in these Information Security Requirements ("**Infosec Requirements**") apply as the baseline set of information security requirements for the handling of Data in connection with Partner's access, processing, or hosting of its and Customers' data, facilities, or systems. For purposes of these Infosec Requirements, "**Data**" includes Confidential Information and all Customer data and information automatically collected by the Collector Technology and Armis Platform or provided to Armis directly by Customer through use of the Armis Platform or via Partner's use of the Armis Platform on behalf of Customer. If Armis revises these Infosec Requirements, it shall provide Partner with reasonable advance written notice and an opportunity to reasonably object to the revised Infosec Requirements. If Armis does not receive a written objection to the revisions before the effective date stated in the notice, Partner will be deemed to have accepted the revisions.

1. General Provisions

a. Partner shall ensure all its personnel working with Data are bound by written confidentiality obligations substantially similar to the confidentiality terms among Armis and Partner in this Agreement. Alternatively, Partner shall sign a corporate non-disclosure agreement which applies to all Partner employees, subcontractors, and vendors who work with Data.

b. Partner shall ensure that any subcontractor or vendor Partner uses in providing any portion of the Services and who is granted access to Data, or access to testing or production of Customers' applications, maintains information security standards at least as comprehensive as those described in these Infosec Requirements. Partner shall maintain updated lists of all such subcontractors, including the agreements it has with such subcontractors detailing such information security standards. Upon written request from Armis, Partner shall share such lists with Armis and if requested by Armis' Information Security Office or Data Privacy Officer and for articulated business reasons, replace any Partner subcontractor whose information security standards/practices are deemed insufficient.

c. In the event Armis provides prior written approval of a subcontractor or vendor, any such subcontractor or vendor must be required to adhere to information security requirements at least as comprehensive as those described in these Infosec Requirements.

d. Partner shall ensure its personnel have passed comprehensive background checks prior to accessing Data, consistent with prevalent information security standards such as ISO27001 and/or SOC2 ("**Infosec Standards**"), and that its personnel's access to Data and/or systems is limited on a need-to-know basis.

e. Partner shall provide adequate training for its personnel periodically, but no less than annually, regarding relevant security, privacy, and business continuity programs. If Partner will access Armis' and/or Armis Customers' systems, if requested, Partner shall require its personnel to complete Armis-provided security and privacy training.

f. Partner shall have security protections defined in these Infosec Requirements across all environments (e.g., production, test, development, etc.) that contain Data.

g. No Armis or Customer Data may be stored, transmitted, accessed, or otherwise sent outside of the geographic territory in which the relevant Armis Affiliate or Customer is located.

h. Any exception to the terms of these Infosec Requirements requires specific, advance written approval from Armis' Information Security Office.

2. Partner's Security Controls and Protections Provisions.

a. Services must be provided with most current and commercially available software and hardware, including, without limitation, operating systems, middleware, databases, servers, laptops, desktops, mobile and other remote devices, etc., or any other software or service the Services are dependent on or used to provide Services. All applicable current security patches must be applied and/or firmware installed and tested for efficacy with the Services.

b. Partner shall provide all security updates to software and supporting software components relevant to Services, at no additional cost to Armis or Customers, in a timely manner, but not to exceed thirty (30) days from when the security updates are commercially available.

c. Without limiting anything set forth in these Infosec Requirements, Partner shall regularly check for and delete viruses and malware in Partner systems used by Partner to provide the Services by way of standard industry virus detection tools.

d. Partner shall not knowingly insert or knowingly allow the insertion into the software of any code which would have the effect of disabling or otherwise degrading all or any portion of the Services.

e. In the event Partner transmits Data to Partner network(s) or system(s), Partner maintains responsibility for properly encrypting the Data over public or wireless networks.

f. Partner shall establish standards for secure transmission, storage, back up and destruction of Data, and provide to Armis, in writing, certification/verification of destruction upon request. Partner shall employ encryption standards that minimally adhere to FIPS 140-2.

g. Partner personnel are prohibited from transmitting Armis and/or Armis Customer Data to portable computing devices such as USB drives, cameras and camera phones, smartphones, and any other portable device that would allow the capturing, printing, or storing of such Data to be exfiltrated.

h. Partner shall encrypt with industry-standard cryptography controls all Partner devices used to access, transmit, or store Data.

i. Partner shall have and maintain procedures consistent with Infosec Standards for managing and containing security incidents which involve Data. If a Partner network is directly connected to networks containing Data, then Partner shall fully involve Armis in its investigation to ensure any incident does not negatively impact Data or Armis or Customer systems. Partner shall also provide Armis, within thirty (30) days of the occurrence of any security incident, with a remediation plan to mitigate the risk of a similar breach from reoccurring.

j. Partner shall cooperate with Armis and any affected Customer in the investigation of any apparent unauthorized access to Partner's systems that affect Data or Partner data relative to the Services performed under this Agreement.

k. Without limiting Partner's obligations as set forth in these Infosec Requirements, if a virus is found in Armis' or Customers' systems due to Partner's Services, then Partner shall notify Armis and any relevant Armis Customers within twenty-four (24) hours and use reasonable efforts to assist Armis or such Customers in reducing the effects of the virus to the extent such virus impacts the systems required for Partner's provisioning Services and, to the extent that the virus causes a loss of operational efficiency or a loss of data, to use reasonable efforts to assist Armis to restore such loss. Partner shall reasonably assist Armis and Armis Customers, as applicable, in resolving a virus in a timely manner, with remediation not to exceed thirty (30) business days from when such virus has been commercially known or reported to Partner by Armis or Armis' Customer.

l. Partner shall employ a vulnerability management program whereby vulnerability scans are performed minimally on a monthly basis and any identified vulnerabilities are timely remediated based on their criticality score. For purposes of vulnerability scoring, Partner agrees that the CVSS score will be used and that the timing of remediation will be as follows:[1]

   i. Critical: Immediately
   ii. High: Within 30 days
   iii. Moderate: within 60 days

[1] If Partner provides software to Armis or an Armis Customer which is utilized to support Medicare-related business, software patches must be made available to fix vulnerabilities as reported by software Partners within seven (7) calendar days for High vulnerabilities, fifteen (15) days for Medium vulnerabilities, and thirty (30) days for Low vulnerabilities.

iv. Low: within 90 days

m. As necessary to provide Services, Partner shall facilitate external connections to the World Wide Web that will have network and host-based, content-based Internet filtering software and other appropriate security controls, including industry standard network and host-based intrusion detection and countermeasures that will detect and terminate any unauthorized activity prior to entering the network and host-based firewalls maintained by Partner.

n. As necessary to provide Services, Partner shall utilize: (i) industry standard firewalls, both network and device (e.g., desktop, laptop, server, and other hosts) based, that regulate all data entering Partner's internal data network from any external source, and which will enforce secure connections between internal and external systems and will permit only specific types of data to pass through; and (ii) industry standard encryption techniques that will be used when Data is transmitted by Partner on behalf of Armis or an Armis Customer.

o. Partner shall, with regards to its authentication, at a minimum require complex passwords to access Data inside a secure working environment.

p. Partner shall provide user identification and access controls designed to limit access to Data to authorized users on a need-to-know basis.

q. Partner shall log and monitor information system access and use continuously. Partner shall perform such logging and monitoring on information systems containing Data, including, at a minimum, registering access ID, time, and authorization granted or denied.

r. Partner shall perform external penetration testing minimally on an annual basis that includes all Internet-facing network and operating system elements that exist between the end-user and the application layer. Partner shall ensure that the application penetration testing is performed by a qualified, independent third party, and Partner is solely responsible for the cost of such testing. Partner shall promptly remediate all noted critical and high-risk vulnerabilities. Partner shall present evidence of compliance with these requirements upon the request by Armis, or as applicable, an Armis Customer.

s. Prior to the effective date of this Agreement and on an annual basis thereafter, Partner shall provide documented responses to a third-party risk management questionnaire provided by Armis, or as applicable, Armis Customer. Completion of a third-party risk management questionnaire by Partner will not constitute an audit under the terms of these Infosec Requirements. Partner shall immediately notify Armis or, as applicable, Armis Customer, as the case may be, of any changes to the answers in the questionnaire that materially and negatively affect the security of Partner Services rendered under this Agreement.

t. Partner shall permit an audit of its privacy and security controls upon reasonable notice.

u. Partner shall periodically audit its personnel who provide services to Armis or Armis Customers to confirm their access rights to Data is appropriate.

3. **Contract Termination**

a. Partner shall have written procedures for the disposal of electronic storage devices, which include instructions for the destruction and sanitization of data.

b. At the conclusion of the engagement, or upon request, Partner shall certify, in writing, that: (i) all Data has been permanently erased from Partner systems, and all subcontractor and downstream recipient(s), systems; or (ii) it has removed the storage device(s) from Partner, and all subcontractor and downstream recipient(s), equipment and provided all such equipment to Armis or Armis Customers who own such Data. In the event Partner will permanently destroy systems pertaining to Services, then Partner shall accomplish the method of destruction by “purging” or “physical destruction”, in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88.

****