Managed Risk Program: Core Essentials

a. Managed Vulnerability Service – Cloud, Co-managed

Managed Vulnerability Service is an eSentire and Client co-managed service which provides access to a vulnerability scan-management and reporting platform and delivers vulnerability reports and vulnerability trending on a predetermined periodic basis, including the following capabilities (the "MVS"):

- Vulnerability Scanning. Vulnerability scanning delivers vulnerability reports and vulnerability trending on a predetermined periodic basis, weekly for external scans and monthly for internal scans to determine Client's vulnerability posture and allow Client to guide network/system configuration and controls. Client also has limited access to co-managed platform to define and direct their own scanning in cooperation with eSentire.
- Vulnerability Reporting. Various reports for external and internal findings are sent by eSentire to Client following each scan. eSentire may also direct Client to reporting platform portal to receive vulnerability reports in addition to or instead of providing scan report findings.
- Monthly Review. Client may request once per month a one hour review of the findings of the scans conducted with an eSentire Information Security Consultant.
- Ad-Hoc Vulnerability Scanning. Client may also direct their own ad-hoc vulnerability scanning via the eSentire-provided vulnerability scan-management and reporting portal with limitations and provided such scanning does not unduly interfere with eSentire delivery of the MVS or other eSentire supplied services.
- This engagement includes weekly external scanning and monthly internal scanning, the quantity of IP Addresses (including cloud-hosted and on-premise assets) set out in the applicable Order Form and which have been provided to eSentire by Client.
- Co-managed service. Client will be provided tenant access to an eSentire-managed scan-management and reporting platform portal. Client may direct their own scans and access reporting independent of eSentire and during this process shall not interfere or otherwise modify agreed scanning policies and scan frequencies as defined by eSentire. Client shall not otherwise interact with the provided tenant access in a manner that adversely affects the delivery of the MVS or any other eSentire-provided Client services with without prior written consent by eSentire.
- Quarterly PCI Attestations. Client may request that eSentire submits external PCI scan results to the approved scanning vendor for PCI-ASV attestation. Such scanning shall be performed a minimum of once per calendar quarter, provided it is Client's sole responsibility to request that scan results are submitted for ASV certification as needed and all required information is provided. It is Client's responsibility to complete a Self-Assessment Questionnaire (SAQ) and assess what level of PCI compliance is required, as well as to provide a complete and accurate scope of assets. The MVS PCI add-on relates to PCI DSS 11.2.2. For the avoidance of doubt, external PCI scans and Attestations of Scan Compliance are not included in the standard MVS offering and additional fees will apply. Quarterly PCI Attestations shall only be provided in connection to the Managed Vulnerability Service.
- Web Application Scanning ("WAS") delivers the ability to scan external facing web applications for known vulnerabilities to determine Client's web application posture and allow Client to guide web configuration and controls. Client also has limited access to co-managed platform to define and direct their own scanning in cooperation with eSentire. For the avoidance of doubt, the Web Application Scanning is not included in the MVS, and additional fees will apply, and the Web Application Scanning shall only be provided in connection to the Managed Vulnerability Service.
- Container Security ("CS") delivers the ability to scan containers for known vulnerabilities to determine Client's container security posture and allow Client to guide container security configuration and controls. Container Security provides detection for container infrastructure and associated applications. Client also has limited

access to co-managed platform to define and direct their own scanning in cooperation with eSentire. For the avoidance of doubt, Container Security is not included in the standard Managed Vulnerability Service offering and additional fees will apply. Container Security shall only be provided in connection to the Managed Vulnerability Service.

Sensors.

eSentire may provide at least one physical or virtual security appliance (a "Sensor") as specified on the applicable Order Form and to the extent required to provide to Client the MVS.

eSentire will configure and remotely manage the Sensor and its embedded software for all devices as part of the MVS. Client may only access the configuration of such Sensor with eSentire's prior written authorization. eSentire shall only access the configuration of other network devices connected to the Sensor with Client's authorization and shall do so through an encrypted and secure means.

Client Responsibilities.

Client is responsible for:

- Any and all data and systems which Client grants access to for receipt of the MVS;
- Obtaining all necessary licenses, permissions, and consents to enable eSentire to access Client's network and servers in order to provide the MVS, including any 3rd party permissions as required;
- Designating a Project Coordinator to work directly with and serve as the primary Client contact with eSentire for the duration of Client receiving the MVS;
- Providing eSentire a complete copy of its security (including privacy) policies, as available. Client is solely responsible for the creation, maintenance, and enforcement of its security policies to protect the security of Client Data and Systems;
- Its choice of equipment, systems, software, and online content;
- Providing the necessary resources, information, documentation and access to personnel, equipment, systems and scanning schedules, as reasonably required by eSentire, to allow eSentire to perform the MVS;
- Notifying eSentire of any change or contemplated change to its network in advance of Client effecting such change;
- Complying with all applicable local, state, provincial, federal, and foreign laws in using the MVS and any provided tools used in conjunction with MVS including but not limited to the vulnerability scan-management and reporting platform portal;
- Advising eSentire of network and IP/endpoint range changes to scope. for the avoidance of any doubt, any material changes to the IP/endpoint count including overages that are greater than a five percent (5%) increase to the contracted scope in any sustained manner greater than 30 days may incur additional costs at the then-current contract rate and shall be calculated by eSentire and billed to Client minus any newly applicable volume discount;

Client responsibilities for Web Application Scanning.

Client is responsible for:

- Specifying one valid Web application address/port for each web application being scanned. Each additional web application being scanned will be billed to Client minus any newly applicable volume discount;
- Accessing WAS service reporting via the eSentire-provided vulnerability scan-management and reporting platform portal;
- Conducting and remediating the found risks and vulnerabilities for each respective Web application;

- Any 3rd party hosting permissions as required.

Client responsibilities for Quarterly PCI Attestations.

Client is responsible for:

- Being proactive towards the remediation of discovered vulnerabilities, contacting eSentire ahead of submission deadlines and in responding to communications regarding PCI compliance;
- Providing all documentation required for their PCI compliance submission a minimum of three weeks before submission, providing updates as required, until documentation is formally submitted; and
- Requesting one scan per calendar quarter so that eSentire submits external scan results to the approved scanning vendor for PCI ASV validation and certification. It is Client's responsibility to request that scan results are submitted for ASV certification as needed.

In the event Client fails to perform its obligations in the time and manner specified or contemplated above, or should any assumption outlined herein with respect to the MVS Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages. In the event that Client fails to notify eSentire of network changes as contemplated above, then eSentire shall be released from any and all obligations to scan Client's network until Client has notified eSentire of such change.

Exclusions.

The MVS excludes the following:

- The design, creation, maintenance, and enforcement of a security policy for Client; and
- eSentire attempting to access Client's servers without Client's express written or verbal consent.

b. Security Program Maturity Assessment

eSentire will review and assess the effectiveness of Client's internal security program against the "Core 15" assessment areas of eSentire's "Cybersecurity Reference Model", other cybersecurity standard(s) or regulatory requirements as may be mutual agreed to by Client and eSentire in writing. The "Core 15" areas of the eSentire Cybersecurity Reference Model include:

- IT Security Strategy & Governance
- Human Resources
- Security Architecture
- IT/Security Risk Management
- Monitoring & Operations
- Incident Response
- Information Management
- Asset Management
- Vulnerability & Patch Management
- Third Party Risk Management
- Compliance & Audit
- Secure Network Design
- Authorization & Access Controls
- Malicious Code Prevention
- Secure Builds

The Security Program Maturity Assessment will also include meetings with appropriate Client designates and subject matter experts, eSentire evaluating risk areas and defining overall risk levels of Client's internal security program, as well as eSentire evaluating and reporting to Client on the quality of Client's processes, routines, and controls. eSentire will provide to Client a baseline assessment of Client's internal security program against eSentire's "Cybersecurity Reference Model", including an executive summary and details findings report in Microsoft Word and Excel formats.

c. Executive Briefings

eSentire will provide an annual executive briefing covering topics such as testing results and subsequent risks, general security trends and the overall threat landscape.