Managed Risk Services

General eSentire Responsibilities for Managed Risk Services. eSentire shall:

a. make available such personnel with requisite technical and project management expertise as required to complete the Managed Risk Services ordered by Client provided that eSentire shall be entitled to supplement or replace such personnel when, in eSentire's judgment, the Managed Risk Services will benefit from such supplementing or replacement; and
b. designate a Project Manager who shall have overall responsibility for the Managed Risk Services ordered by Client and who shall interface with Client's Project Coordinator.

If not already in place, and if required, eSentire will provide one physical security appliance (a "**Sensor**") as agreed to prior to the start of the configuration of such Sensor. Such locations shall be listed within the Required Configuration and Shipping Information. On execution of the Order Form, eSentire shall configure the Sensor(s) for shipment to Client.

Sensor(s) will be deployed to analyze network traffic flows of the following types:

a. External Network (Internet) to Internal Network;
b. Internal Network to External Network (Internet); and
c. Other data segments, depending on the requirements.

General Client Responsibilities for Managed Risk Services. Client is responsible for:

a. providing eSentire with reasonable access to Client's IT infrastructure, including without limitation:
   - a copy of Client's relevant IT policies and procedures;
   - access to members of Client's IT staff upon request by eSentire; and
   - any other resources that eSentire may reasonably request that can be readily compiled or supplied by Client without significant cost or labor.
b. any and all data and systems which Client grants access to for receipt of the Managed Risk Services;
c. obtaining all necessary licenses, permissions, and consents to enable eSentire to access Client's network and servers in order to provide the Managed Risk Services;
d. designating and maintaining a Project Coordinator to work directly with and serve as the primary Client contact with eSentire for the duration of Client's receipt of the Managed Risk Services from eSentire;
e. creating, maintaining, and enforcing its security policies to protect the security of Client Data (including any Personal Information), its computer network and other systems and facilities (collectively, "Client Data and Systems");
f. its choice of equipment, systems, software, and online content;
g. complying with all applicable local, state, provincial, federal, and foreign laws in receiving the Managed Risk Services;
h. providing accurate IP addresses to eSentire; and
i. prior to eSentire commencing the Managed Risk Services, notifying eSentire of all unique or non-standard system and application characteristics of Client's systems, or of any system, application, or equipment modifications known or suspected to be potential problems, or deviations from industry standard practices (for example, unique testing procedures, naming conventions, user exits, local code modifications or custom implementations).

Should Client fail to perform its obligations in the time and manner specified or contemplated above, or should any assumption set out herein with respect to the Managed Risk Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages.

Client hereby represents and warrants to eSentire, and acknowledges eSentire's reliance on such representation and warranty, that all IP addresses provided to eSentire are owned, operated, licensed or controlled by Client and or its employees, consultants or authorized agents. eSentire is not liable for any losses, liabilities, damages, fines, penalties, deficiencies, costs or expenses, including the reasonable fees and reasonable expenses of legal counsel, accountants or other experts and professional advisers, arising from or relating to any incorrect IP address information provided to eSentire in connection with its provision of the Managed Risk Services.

In the event testing of any IP address not owned by Client is required, Client shall provide prior notice to eSentire and have secured all necessary consents, permissions and waivers from the owner of the IP addresses prior to eSentire performing any testing.

Place of Performance.

eSentire shall perform the Managed Risk Services remotely whenever possible.

Travel and Related Expenses.

If at the request and with approval of Client eSentire personnel is required to provide Services at Client premise or any location designated by Client, eSentire shall be reimbursed for reasonable travel and related expenses in addition to the fees for Managed Risk Services as described in an Order Form. Such reimbursement shall be made for normal expenses directly attributable to the Services provided herein. An itemized receipt shall be produced by eSentire as backup to document actual expenses incurred upon request of Client.

Reports.

If applicable, eSentire will provide to Client an executive summary of the scope, approach, findings and its recommendations in connection with the Managed Risk Services provided to Client. If applicable, eSentire will provide a technical report including, but not limited to, the methodology employed, positive security aspects identified by eSentire, detailed technical findings, and, in eSentire's opinion, risk rating of vulnerabilities identified by eSentire accompanied by exhibits of such vulnerabilities, in each case, when appropriate. eSentire may also provide, if applicable, technical remediation steps connection with the Managed Risk Services provided to Client. Client may, upon request, discuss the findings of such reports with eSentire.

Services Description.

Managed Risk Services include the list of cybersecurity program support services (see below list and see landing page link to services) related to the creation, oversight, and implementation of Client's formal cybersecurity program, as well as assessing such program's effectiveness, and providing security consulting services related to supporting the security of Client's IT infrastructure (collectively, "**Managed Risk Services**"). Client may order one or more of the following Managed Risk Services by executing an Order Form:

- Technical Testing - External Vulnerability Scan and Penetration Test
- Technical Testing - Internal Penetration Testing
- Technical Testing - Web Application Testing
- Technical Testing - Managed Phishing and Security Awareness Training (Co-managed)
- Technical Testing - Managed Phishing and Security Awareness Training (Essentials Package)
- Virtual CISO - Security Program Maturity Assessment
- Cyber Risk Advisor Services
- Virtual CISO - Security Incident Response Planning
- Security Policy Review and Guidance
- Security Architecture Review
- Virtual CISO - Vendor Risk Management Program
- Virtual CISO - Vulnerability Management Program

- Managed Endpoint Defense
- Managed Vulnerability Service – Cloud, Co-managed.
- Managed Risk Program: Core Essentials
- Managed Risk Program: Measure and Engage
- Managed Risk Program: Mature and Direct
- Managed Risk Program: Harden and Wargame