CI-SOC Alliance Membership Agreement

(Version 1.0)

Upon completion in full, please send a signed copy of this agreement in PDF form by email to CISOC@cybernb.com and an invoice will be sent to you for the membership fee. A countersigned copy of this application will be returned to you for your records when your eligibility for membership has been confirmed.

This Membership Agreement is made effective as of _____, 20__ (the "**Effective Date**") by and between CyberNB Inc. ("**CyberNB**"), a New Brunswick, Canada corporation, and _____ (the **"Member**"), a _____ corporation. CyberNB and the Member are collectively referred to herein as the "Parties".

APPROVED MEMBERSHIP LEVEL

Membership Level	**Annual Fee**
● Platinum	$50,000
○ Gold	$25,000
○ Silver	$12,000
○ Bronze	$6,000

WHEREAS, the mission of the CI-SOC Alliance is to achieve optimal cybersecurity critical infrastructure protection and resiliency through collaboration amongst an alliance of industry, government, and academia partners.

WHEREAS, the undersigned agrees to become a Member of the CI-SOC Alliance at the membership level selected and be subject to the rights and obligations of members set forth in this agreement and the CI-SOC Alliance Cyber Intelligence Exchange Agreement.

WHEREAS, the current feature set for the membership level selected includes:

Threat Detection & Sharing Service	**Bronze**	**Silver**	**Gold**	**Platinum**
Multi-tenant, supported, federated threat intel sharing platform	✓	✓	✓	✓
Alliance member-to-member threat intel sharing & collaboration	✓	✓	✓	✓
MITRE ATT&CK threat intel repository integration and support	✓	✓	✓	✓
CCCS, CanCyber, & open source threat intel data feeds	✓	✓	✓	✓
Multi-tenant, supported, collaboration management platform	✓	✓	✓	✓
Multi-tenant, supported, knowledge management platform	✓	✓	✓	✓

Risk Advisory & Assessment Service				
EBIOS Risk Manager methodology & Agile RM software		✓	✓	✓
EBIOS Risk Manager and Agile Risk Manager training & support		✓	✓	✓
Cybersecurity standards, regulations, & frameworks support		✓	✓	✓

Cybersecurity Marketplace Service

Member products & services marketplace, co-marketing, co-selling			✓	✓
Provincial, national, & international opportunities			✓	✓
Cyber supply arrangement			✓	✓
Cyber Park fusion centre seats			✓	✓

IN WITNESS WHEREOF, the Parties have executed this agreement on the date as set forth below.

CyberNB:	**Member:**
By:	By:
Print Name:	Print Name:
Title:	Title:
Date:	Date:

Financial Contact
Please identify Member financial contact for invoice submission.

Name:
Title:
Address:
Email Address:

CI-SOC Cyber Intelligence Exchange Agreement

(Version 2.b)

This CI-SOC Cyber Intelligence Exchange Agreement ("**Agreement**") is entered into by the CyberNB Inc and the entities listed on the signature pages below (collectively, "**Members**"; together with CyberNB Inc, the "**Parties**" and each separately a "**Party**") for the purpose of facilitating the exchange of certain cybersecurity-related data, analytics, information and intelligence (collectively "**Cyber Intelligence**") and Methods for use in a CyberNB Inc-led multi-phased initiative to collaboratively develop, implement and operate a cross-sector critical infrastructure security operations centre ("**CI-SOC** ").

Whereas the goal of the CI-SOC is to: (i) proactively collect, normalize and correlate Cyber Intelligence relating to critical infrastructure assets on a cross-sectoral basis, (ii) share and contextualize such Cyber Intelligence, and formulate new Cyber Intelligence and Methods to help mitigate cyber threat risks, prevent imminent cyber-attacks, contain, disrupt and eliminate actual cyber-attacks, and to coordinate the collaborative recovery from critical infrastructure breaches, and (iii) lay the foundations to establish an ongoing cross-sector critical infrastructure security operations centre based on the CI-SOC deliverables and (iv) provide an analytical sensor array that is easily deployed via standard and modern computing technologies and (v) deliver an analytical fabric that provides insight into ongoing/current/past/future attacks ((i), (ii), (iii), (iv) and (v) collectively, the "**Purpose**");

Whereas a key requirement of the CI-SOC is to gain access to qualified Cyber Intelligence from security information and event management ("**SIEM**") systems, and eventually from other security operation centre tools, that identify and characterize cybersecurity events being encountered by critical infrastructure operators;

Whereas the CI-SOC intends to combine the Cyber Intelligence it gathers from Members, with Cyber Intelligence it gathers from government and threat intelligence services, to form a regional, multi-sector, critical infrastructure-focused Cyber Intelligence repository ("**Cyber Intelligence Repository**");

Whereas the CI-SOC P intends to mine the Cyber Intelligence Repository using state-of-the-art cybersecurity advanced analytics tools and methods, along with new methods developed through related research, with the objective of improving the speed and effectiveness of critical infrastructure cyber threat detection, correlation, analysis and characterization, and threat prevention and incident response;

Whereas the CI-SOC results, including access to Cyber Intelligence and Methods, and to the production version of the Cyber Intelligence Repository itself, will be shared with Members SOCs as part of the CI-SOC coordination of regional collaborative responses to cyber threats and attacks, for use in association with Members' customers who own or operate the critical infrastructure assets that are a source of the cyber data and information used in the CI-SOC ;

Whereas the archival versions of the Cyber Intelligence Repository will be shared with all Members to facilitate the research, development and testing of advanced analytics and new cybersecurity threat detection products and services;

Whereas the Parties acknowledge that sharing of Cyber Intelligence will require protecting the identity of critical infrastructure owners or operators, as well as their system and cybersecurity architecture designs and vulnerabilities, and any other sensitive and/or personal information;

Now therefore in consideration of the mutual covenants and data entitlements herein, the Parties agree as follows:

1.0 DEFINITIONS

1.1 **Definitions.** In this Agreement:

(a) "**Affiliate**" means a corporation, company, division or other entity directly or indirectly owned or controlled by, or under common control of, the same ultimate parent company as a Party, and will include the ultimate parent company.

(b) "**Member SOC**" means a Member who uses a security operations centre (SOC) to provide cyber threat, attack and breach detection, containment and elimination services to owners and operators of critical infrastructure assets;

(c) "**Applicable Law**" means any applicable law, rule, regulation, order, or other action, decree, requirement, or guideline published or in force at any time during the term of this Agreement which governs or regulates any

Party, or any Affiliate or CI Customer thereof, including laws governing the handling of information about identifiable individuals ("**Privacy Laws**");

(d) "**CI Customer**" means a customer of a Member who owns or operates critical infrastructure assets that are monitored by the Member for Threats and who has authorized the Member to share its Threat Intelligence related to its critical infrastructure assets with the CI-SOC under the terms of this Agreement;

(e) "**CI-SOC Cyber Intelligence Data Feed**" means an automated, trusted, unidirectional or bidirectional data feed provisioned by the CI-SOC Operator to transmit Cyber Intelligence between the CI-SOC Operator and Members, government and threat intelligence services;

(f) "**CI-SOC Steering Committee**" refers to the delegates from Platinum Members that collaborate with CyberNB Inc to review the mandate and operations of CI-SOC on a periodic basis.

(g) "**CI-SOC Operator**" is defined in Section 2.1 (CI-SOC Operator);

(h) "**Confidential Information**" means, subject to the exceptions specified in the Operating Model or in Section 4.1 (Confidentiality) below, the Data Broker (including associated design details and documentation), and all Contributed Cyber Intelligence & Methods and Cyber Intelligence & Methods;

(i) "**Confidentiality Period**" means the time period during which Recipient is required to maintain the obligations of confidentiality and limited use defined in this Agreement. The Confidentiality Period: (i) for the Data Broker will continue for the life of any associated Intellectual Property; and (ii) for all other Confidential Information, including any Contributed Cyber Intelligence & Methods and Cyber Intelligence & Methods, will be 5 years after termination of the Disclosure Period;

(j) "**Contributed Cyber Intelligence & Methods**" is defined in Section 2.3 (Reporting Cyber Intelligence). For greater certainty, it includes any Threat Intelligence, Threat Information and Methods made available by third parties to, or produced by or for, the CI-SOC Operator for use in CI-SOC;

(k) "**Cyber Intelligence**" is defined in the recitals of this Agreement;

(l)"**Cyber Intelligence & Methods**" is defined in Section 2.5(e). For greater certainty, it includes Cyber Intelligence and Methods created, derived or formulated by or for the CI-SOC Operator specifically for the identification, analysis or communication of Threats or Incidents, as well as correlated Cyber Intelligence (including Contributed Cyber Intelligence & Methods) sourced from Members, government, threat intelligence services and other cyber intelligence sources;

(m) "**Cyber Intelligence Repository**" is defined in the recitals of this Agreement. For greater certainty, it includes all Contributed Cyber Intelligence & Methods, and all other Cyber Intelligence and Methods generated by mining activities authorized pursuant to the terms of this Agreement;

(n) "**Data Broker**" means software provisioned by the CI-SOC Operator to Members to collect, normalize and anonymize Cyber Intelligence provided by Members;

(o) "**Discloser**" means a Party that disclose(s) Confidential Information to another Party (or Parties) under this Agreement;

(p) "**Disclosure Period**" means the time period during which any disclosure of Confidential Information binds the Parties under the terms of this Agreement. The Disclosure Period for this Agreement will begin on the Effective Date and will terminate as of the applicable Termination Date;

(q) "**Effective Date**" means May 1st, 2019;

(r) "**Incident**" means an occurrence of one or more security events that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system, or the data the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies;

(s) "**Intellectual Property**" of "**IP**" means any and all proprietary rights in technology recognized in any jurisdiction in the world, including: (i) rights associated with works of authorship, databases and software, including copyrights and moral rights; (ii) trade secrets and confidential information rights; (iii) patent rights, patents, designs and other industrial property rights; (iv) all other intellectual and industrial property rights, however designated; and (v) all registrations, priority rights, initial applications, renewals, extensions, continuations, divisions, reissues, and associated rights relating to any of the foregoing rights;

(t) "**Methods**" means the procedures, techniques, plans and strategies used to detect, prevent, contain, eliminate, assess impact, and recover from cyber threats and attacks;

(u) "**Operating Model**" is defined in the recitals of this Agreement. For greater certainty, it will include the Cyber Intelligence Policy and scope of processes, programs, procedures and controls approved by the Executive of CyberNB Inc. for each CI-SOC Release to be implemented by the CI-SOC Operator and the Members to protect the security, integrity and accuracy of Contributed Cyber Intelligence & Methods and of the Cyber Intelligence Repository. These include policies relating to the gathering, structuring, correlating, filtering, obfuscating, accessing, communicating, processing, storing, use and protection of such Cyber Intelligence.

(v) "**Personal Information**" means information of a personal or sensitive nature that can be used on its own or with other information to identify, contact or locate a natural person;

(w) "**Personnel**" means directors, officers and employees of, and individual contractors providing staff augmentation support to, a party or any of its Affiliates;

(x) "**Recipient**" means a Party (or Parties) that receives Confidential Information under this Agreement;

(y) "**Regional Incident**" means an Incident declared by the CI-SOC to be a major, regional, multi-CI organization, cyber-related security event affecting critical infrastructure, deemed to require a coordinated, collaborative, regional incident response.;

(z) "**Regional Threat**" means a Threat declared by the CI-SOC to be a major cyber-related security threat to critical infrastructure in a region and that is deemed to require a coordinated, collaborative, regional threat prevention response aimed at preventing a cyber attack on critical infrastructure;

(aa) **"Security Event**" means a security event that actually or potentially jeopardizes the confidentiality, integrity or availability of critical infrastructure, or that constitutes a violation or imminent threat of violation of applicable security policies, security procedures or acceptable use policies;

(bb) "**Security Event Alert**" means a notification of a Security Event;

(cc) "**Sighting**" means an observation or indicator of a potential forthcoming Incident. Sightings are used to track who and what is being targeted, how attacks are carried out and trends in attack behaviour;

(dd) "**Termination Date**" means in respect of a Party, the date of termination of their participation as a Party to this Agreement;

(ee) "**Threat**" means anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage or destroy an asset. Threats are not necessarily confirmed (commonly referred to as a "false positive") and may be inferred, perceived or be an actual and direct threat;

(ff) "**Threat Information**" means information related to a Threat that might help an organization protect itself against a Threat or detect malicious activities. Major types of Threat Information include indicators of attack ("**IOA**"), indicators of compromise ("**IOC**"), tactics, techniques and procedures ("**TTPs**"), Security Event Alerts, Threat Intelligence reports and tool configurations.

(gg) "**Threat Intel Briefing**" means a prose document that describes a cyber Threat, and associated Threat Information and Threat Intelligence. It includes: IOAs, IOCs, threat actors, nation-states, attack patterns, Sightings, vulnerabilities and TTPs. Threat Intel Briefings are a key means to communicate and exchange Threat Intelligence between the CI-SOC Operator, Members, external partners and other external organizations and services;

(hh) "**Threat Intelligence**" means Threat Information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes;

(ii) "**Use**" means to use, copy (but only as necessary for authorized purposes) adapt, modify, translate, , abridge, condense, filter, edit, expand, combine, compile, derive information or works from (including by application of arithmetical, logical or algorithmic processes), evaluate, analyse, test, visualize, represent, exercise, install, transfer (including by telecommunicating or posting for secure download), operate, maintain, manage, support, repair or otherwise process;

(jj) "**Validated Incident**" means an Incident that includes one or more validated security events wherein an Member SOC has confirmed that one of its client's critical infrastructure systems or data have been attacked or compromised; and

(kk) Other capitalized terms defined in any part of this Agreement will have their indicated meaning throughout this Agreement.

2.0 CYBER INTELLIGENCE EXCHANGE

2.1 **CI-SOC Operator.** References to any rights or obligations of the "**CI-SOC Operator**" in this Agreement will be interpreted as rights or obligations of CyberNB, except to the extent that any rights or obligations of the CI-SOC Operator have been delegated by the CI-SOC Steering Committee to a separate entity established to assume the ongoing responsibilities of an ongoing CI-SOC operation ("**Production CI-SOC Operator**"). Except to the extent of such delegation, all decisions of CyberNB Inc.(as the CI-SOC Operator) relating to its rights and obligations under this Agreement will be made in accordance with the Plan, the terms of this Agreement and such other directions provided by the CI-SOC Steering Committee from time to time. For greater certainty, the production CI-SOC operation may be launched in parallel with the ongoing development of CI-SOC Releases and will adopt CI-SOC Release developments as and when approved by the CI-SOC Steering Committee.

2.2 **Data Broker and Cyber Intelligence Data Feed.** The CI-SOC Operator will provision: (i) software to Members to normalize and anonymize Cyber Intelligence elements of Contributed Cyber Intelligence & Methods, and (ii) a CI-SOC Cyber Intelligence Data Feed to transit Cyber Intelligence elements of Contributed Cyber Intelligence & Methods to the CI-SOC Operator for subsequent processing and storage in the CI-SOC Cyber Intelligence Repository, in each case in accordance with the applicable CI-SOC Release schedules and the corresponding specifications defined by the Operating Model.

2.3 **Contributed Cyber Intelligence & Methods.** Subject to the terms of this Agreement, including the agreed-to form and scope of Cyber Intelligence exchange for each CI-SOC Release (as specified in the Operating Model), each Member will provide at its earliest opportunity to the CI-SOC Operator for Use for the Purposes of the CI-SOC , notice of and all available Threat Information, Threat Intelligence and Methods relating to all Validated Incidents, Sightings, Security Event Alerts, Security Events and other events specified in the Operating Model as contributing events (collectively, "**Contributed Cyber Intelligence & Methods**") identified by the Member (including for any CI Customers).

2.4 **Anonymized Data.** Members will use the Data Broker, or Member-provisioned manual procedures or tools, to ensure that Cyber Intelligence elements of Contributed Cyber Intelligence & Methods have been filtered or modified to remove or obfuscate all: (i) Personal Information, including any Personal Information relating to its Personnel, the Personnel of its suppliers, subcontractors or CI Customers, and Personal Information of its CI Customers' clients' Personnel and its and their clients or end-users; and (ii) Confidential Information of the Member, or its suppliers, subcontractors, CI Customers, or their clients or end-users, that could be used to identify the origin of the Contributed Cyber Intelligence & Methods.

2.5 **Use of Contributed Cyber Intelligence & Methods.** The CI-SOC Operator is authorized to and will use Contributed Cyber Intelligence & Methods solely in accordance with the Operating Model and for the Purposes of the CI-SOC , which include the following:

(a) to filter, normalize and correlate Cyber Intelligence elements of Contributed Cyber Intelligence & Methods for the purpose of collecting, processing, structuring and storing it in the Cyber Intelligence Repository with other CI-SOC-generated Cyber Intelligence and Cyber Intelligence sourced from government, threat intelligence services and other sources;

(b) to share Methods and anonymized versions of the Cyber Intelligence elements of Contributed Cyber Intelligence & Methods (wherein any information that could be used to associate Contributed Cyber Intelligence & Methods with the contributing Member has been removed or obfuscated in accordance with the specifications defined in the Operating Model for the applicable CI-SOC Release level) with all Members for use in association with their own Threat detection products and services for the benefit of their CI Customers;

(c) to correlate and analyse Cyber Intelligence elements of Contributed Cyber Intelligence & Methods, formulate new or enhanced Cyber Intelligence using advanced analytics, and formulate new or enhanced Methods, in isolation or in combination with all or part of the Cyber Intelligence Repository, to detect cyber threats, attacks and breaches;

(d) subject to the terms of this Agreement, including the agreed-to form and scope of Cyber Intelligence and Methods exchange for each CI-SOC Release (as specified in the Operating Model), to provide at its earliest opportunity to Members for Use in association with their own Threat detection products and services for the benefit of their CI Customers, notice of, and all Threat Information, Threat Intelligence and Methods relating to all Regional Threats and Regional Incidents (collectively, "**Regional Cyber Intelligence & Methods**")identified by the CI-SOC Operator;

(e) to use the Cyber Intelligence Repository for the purpose of developing, validating and optimizing new or enhanced methods and tools for Threat detection and response, and to assess the effectiveness of third-party methods and tools;

(f) to provide access to the Cyber Intelligence Repository to Member SOCs for the purpose of enhancing its Threat detection and response capabilities of its products and services on behalf of its CI Customers; and

(g) to create and share an anonymized archival version of the Cyber Intelligence Repository (wherein any information that could be used to associate Contributed Cyber Intelligence with contributing Member has been removed or obfuscated in accordance with the specifications defined in the Operating Model) with all Members for the purpose of developing, validating and optimizing new or enhanced methods and tools for Threat detection and response.

2.6 **Subcontracting.** The delegating or subcontracting of all or any part of a Party's obligations set out in this Agreement to any Affiliate, supplier or subcontractor ("**Subcontractor**") will not relieve the Party from any obligation or liability under this Agreement. The Party will remain responsible for the performance of all or any part of its obligations set out in this Agreement performed by Subcontractors and for any act or omission by any Subcontractor to the same extent as if the performance, act, or omission was the Party's performance, act, or omission. The subcontracting Party will ensure that each Subcontractor performs any of the Party's obligations set out in this Agreement that have been delegated or subcontracted to the Subcontractor.

2.7 **Personal Information.** If any Personal Information is inadvertently obtained from a Party by the CI-SOC Operator, or any other Party, the Party who received the Personal Information will: (i) comply with all Privacy Laws applicable to the Personal information; and (ii) immediately notify the Party who disclosed the Personal Information of its receipt, in which case the disclosing Party will instruct receiving Party on the prompt return or destruction of the Personal Information. If disclosure of Personal Information to the CI-SOC Operator becomes necessary for the Purpose, and the disclosing Members are willing and able to provide such information for use in the CI-SOC , then before receiving or having access to such information, the Parties will enter into an amendment to this Agreement that addresses the use and protection of Personal Information in accordance with Applicable Laws (including Privacy laws) and the disclosing Parties' use and security requirements.

3.0 INTELLECTUAL PROPERTY

3.1 **Intellectual Property.**

(a) All Members (and their licensors) will retain all right, title and interest (including all Intellectual Property rights) in and to their respective Contributed Cyber Intelligence & Methods.

(b) Subject to Section 3.1(a), the CyberNB Inc.will retain all right, title and interest (including all Intellectual Property rights) in and to the Cyber Intelligence Repository, all Regional Cyber Intelligence & Methods, and all other Cyber Intelligence and Methods created, derived or formulated by or for the CI-SOC Operator specifically for the identification, analysis or communication of Threats or Incidents .

(c) Each Member hereby grants to CyberNB Inc.a non-exclusive, irrevocable, paid-up and royalty free worldwide license under their Intellectual Property to Use in accordance with the terms of this Agreement (including the Operating Model) their Contributed Cyber Intelligence & Methods solely for the Purpose, including all of the activities specified in Section 2.5 (Use of Contributed Cyber Intelligence & Methods). CyberNB's license rights are perpetual, will survive termination of this Agreement for any reason, and include the right to sublicense its rights to Members, and to the Production CI-SOC Operator, solely for the Purposes contemplated in Section 2.5 and in accordance with the Operating Model and any directions provided by the CI-SOC Steering Committee from time to time. CyberNB Inc.will remain responsible for any act or omission by its sublicensees to the same extent as if the act or omission was CyberNB's act or omission.

(d) CyberNB Inc.hereby grants to each Member SOC until their Termination Date a non-exclusive, revocable, paid-up and royalty free worldwide license under CyberNB's Intellectual Property, and sublicense under the CI-SOC Operator's license rights granted to CyberNB Inc.in Section 3.1(c) above, to Use in accordance with the terms of this Agreement (including the Operating Model) the Cyber Intelligence & Methods and the Cyber Intelligence Repository (to the extent made available to Member SOCs under the Operating Model) solely for the Purpose and in association with their own Threat detection products and services for the benefit of their CI Customers. For greater certainty, this license grant does not include any sublicensing rights, and any authorized copying of the anonymized archival version of the Cyber Intelligence Repository is strictly limited to that necessary to use the licensed Cyber Intelligence and Methods for the expressly authorized purpose.

(e) CyberNB Inc.hereby grants to each Member until their Termination Date a non-exclusive, revocable, paid-up and royalty free worldwide license under CyberNB's Intellectual Property to Use in accordance with the terms of this

Agreement (including the Operating Model) an anonymized archival version of the Cyber Intelligence Repository (to the extent made available to Partners under the Operating Model) solely for the purpose of internally developing, validating and optimizing new or enhanced methods and tools for Threat detection and response. For greater certainty, this license grant does not include any sublicensing rights, and any authorized copying of the anonymized archival version of the Cyber Intelligence Repository is strictly limited to that necessary to use the licensed Cyber Intelligence for the expressly authorized purpose.

(f) All licenses not expressly granted in this Section 3 are reserved and no other licenses, immunity or rights, express or implied are granted, by implication, estoppel, or otherwise.

4.0 SECURITY

4.1 **Confidentiality.**

(a) Obligations of Confidentiality. The Parties agree to maintain in confidence and not to disclose, directly or indirectly, to any person, firm, corporation or other entity whatsoever except as expressly permitted herein any Confidential Information (whether verbal, written or stored or communicated in any other form or medium whatsoever) or use any Confidential Information for any purpose other than: (i) for the Purpose in association with CI-SOC , (ii) in association with its own Threat detection products and services for the benefit of its CI Customers, or (iii) for other purposes expressly authorized by the Operating Model ((i), (ii) and (iii) collectively, the "**Business Purpose**"). Verbal or visual disclosures will be deemed Confidential Information from the date of the disclosure.

(b) Permitted Disclosure of Confidential Information and Limited Use. Notwithstanding anything else, herein, a Recipient is entitled to disclose Confidential Information to its own and its Affiliates' employees, officers, or directors, contractors and legal counsel heretofore referred to as "**members of the organization**", provided that:

(i) such party has a need to know such Confidential Information as required to accomplish the Business Purpose;
(ii) the Recipient will inform such members of the organization of the confidential and proprietary nature of the Confidential Information;
(iii) such members of the organization are bound by obligations of confidentiality no less restrictive than those set forth in this Agreement; and
(iv) the Recipient will be responsible for any breach of this Agreement by any members of the Recipient's organization.

(c) Remedies. The Parties acknowledge that a breach of this Agreement may result in immediate and irreparable harm to the CI-SOC Operator and/or one of more Members or their CI Customers, which money damages cannot adequately remedy. Accordingly, the Parties agree that the CI-SOC Operator or any Member threatened by a breach of this Agreement will be entitled to seek an injunction to prevent any such breach.

(d) Exclusions. It is understood that the confidentiality obligations contained herein are subject to any disclosure required by law. It is also understood that Confidential Information will not include any information or data if a Recipient can show that such information:

(i) is expressly declared not to be Confidential Information in the Operating Model;
(ii) was part of or became part of the public domain provided that such information did not enter the public domain as a result of a breach of this agreement or a breach of any similar confidentiality obligations owed to the CI-SOC Operator or an Member by another party;
(iii) was rightfully in Recipient's or members of the organization's possession prior to receipt from Discloser;
(iv) becomes rightfully available to Recipient or members of the organization from a source other than Discloser who is free to lawfully disclose such information to Recipient members of the organization;
(v) is approved for release by written agreement of Discloser; or
(vi) is independently developed by Recipient members of the organization, as evidenced by written records, without the use of Discloser's Confidential Information.

Confidential Information will not be deemed to be in the public domain merely because any part of the Confidential Information is embodied in general disclosures or because individual features, components or combinations thereof are known or become known to the public. Lastly, it is understood that the disclosure of Confidential Information to other persons who have also entered into this Agreement will not be considered a

breach of this Agreement provided that such disclosure is made only for the purpose of properly participating in the CI-SOC . The Parties agree that any such disclosure will be on a need to know basis only.

(e) Disclosures Required by Law. If Recipient is required by a court or federal, provincial or local agency to disclose Confidential Information, Recipient will, where permissible by law, promptly notify Discloser of such order and reasonably cooperate with the Discloser, where desired by the Discloser, to seek a protective order or take any other action as it deems appropriate. In such circumstances, the Recipient will exercise all reasonable efforts to disclose only the minimal amount of Confidential Information required to satisfy such order. Recipient acknowledges that any disclosure of Confidential Information may result in significant financial loss to Discloser and would potentially harm Discloser's competitive and negotiation positions or may otherwise have a negative impact on Discloser's commercial interests. To the extent the Recipient is required to respond to an access for information request, Discloser requires the right to identify commercially sensitive and confidential information, in accordance with law. Accordingly, Recipient will promptly inform Discloser of such a request and will assist Discloser in claiming an exemption and objection to disclosure.

(f) No Further Obligation. Neither the receipt of Confidential Information nor discussions held in connection with any Business Purpose will prevent a Party from pursuing similar discussions or transactions with third parties, or obligate a Party to continue discussions with the other Party or to take, continue or forego any action relating to the Business Purpose unless otherwise expressly agreed by the Parties in writing. Provided the confidentiality obligations outline in this Agreement are maintained, the receipt of Confidential Information under this Agreement does not preclude the Recipient from developing, manufacturing, marketing or providing products or services which may be competitive with products or services of the Discloser, or entering into any business relationship with any other party. Nothing in this Agreement limits the parties' ability to assign its employees to other s. Experience naturally acquired by a Party's employees (or subcontractors) during the course of the Parties' relationship may be utilized in its business activities and such utilization does not violate this Agreement. Any proposals, estimates or forecasts provided by Discloser to Recipient will not constitute commitments.

4.2 **Controls and Audit.**

(a) Controls. Each Party will implement the procedures required by the Operating Model to monitor and report on compliance with the restrictions and information security requirements of the Operating Model and comply with the terms of this Agreement ("**Control Framework**"). To the extent available, a Party will promptly demonstrate to the CI-SOC Operator, and to other Parties, upon written request its compliance with its Control Framework via a compliance certification or similar document ("**Compliance Report**") issued by an independent auditor: (i) on the suitability of the Control Framework design, (ii) whether the Control Framework has been implemented, and (iii) the operating effectiveness of the Control Framework to meet industry standard criteria for security, confidentiality, integrity and privacy principles.

(b) Audit. If a Party has not provided a Compliance Report as set out in Section (4.2(a) within thirty (30) days, or if the Compliance Report provided fails to satisfy mandatory requirements under Applicable Law, then the requesting Party will have the right to have an independent, internationally accredited, external auditor perform an audit of the requested Party's Control Framework. Audits will be at the at requesting Party's expense and may not be requested more than once per calendar year. Audits will be announced in advance by the requesting Party providing notice in writing to the requested Party no less than one hundred and twenty (120) days prior to the audit date. As part of the notice, the requesting Party must provide its proposed audit requirements (including details regarding audit scope) for consideration. The audit scope may not exceed the mandatory requirements under Applicable Law. The Parties will cooperate with each other in planning and conducting such audits. The requesting Party will act reasonably in conducting such audits, considering the nature of the Control Framework and the environment in which it has been implemented, in order to minimize the impact on the requested Party's operations. The requesting Party's auditors will be supervised by the requested Party while conducting the audit. An audit may not exceed five (5) consecutive business days and must be conducted during the requested Party's regular business hours. Any audit report, notes or other documentation relating to an audit ("**Audit Results**") will be the requested Party's Confidential Information.

5.0 REPRESENTATIONS AND WARRANTIES

5.1 **Limited Representation and Warranty.** Each Member represents and warrants to the CI-SOC Operator and to each other Party that it has obtained from any third party involved in the creation of, or whose Intellectual Property of Confidential Information forms part of, the Member's Contributed Cyber Intelligence & Methods, all necessary written consents to ensure the CI-SOC Operator, the Members, and any person claiming a right or interest in the Cyber Intelligence or the Cyber Intelligence

Repository through the CI-SOC do not infringe any third party Intellectual Property rights or misappropriate any third party confidential information. Notwithstanding this limited warranty, the Parties understand that no other assurances are provided by any Party, its Affiliates or their Personnel that the Contributed Cyber Intelligence & Methods, or the Cyber Intelligence Repository does not infringe the Intellectual Property rights of any other entity.

5.2 **Warranty Disclaimer**. EXCEPT AS EXPRESSLY PROVIDED IN SECTION 5.1 (LIMITED REPRESENTATION AND WARRANTY), THE CONTRIBUTED CYBER INTELLIGENCE & METHODS, REGIONAL CYBER INTELLIGENCE & METHODS, AND CYBER INTELLIGENCE REPOSITORIES ARE PROVIDED ON AN "AS IS" BASIS AND WITHOUT REPRESENTATION OR WARRANTY OF ANY KIND AND WITHOUT ANY VERIFICATION AS TO ACCURACY, SUITABILITY OR COMPLETENESS. THE PARTIES, AND THEIR AFFILIATES, SUBCONTRACTORS AND CI CUSTOMERS, (COLLECTIVELY REFERRED TO AS THE "PARTY" FOR THE PURPOSES OF THIS SECTION 5.2 (WARRANTY DISCLAIMER) AND SECTION 6.0 (LIMITATION OF LIABILITY)) EXPRESSLY DISCLAIM ALL REPRESENTATIONS, WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES AND CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Each Party is solely responsible for determining the appropriateness of using and distributing the Contributed Cyber Intelligence & Methods, Regional Cyber Intelligence & Methods and/or Cyber Intelligence Repositories and assumes all risks associated with its exercise of license rights and entitlements under this Agreement, including the risks and costs of errors, compliance with Applicable Laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6.0 LIMITATION OF LIABILITY

6.1 **Limitation of Liability.**

EXCEPT TO THE EXTENT SUCH A LIMITATION IS PROHIBITED BY LAW, IN NO EVENT WILL ANY PARTY BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES ARISING OUT OF OR RELATING TO THIS AGREEMENT, WHETHER UNDER A THEORY OF CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCTS LIABILITY, OR OTHERWISE, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY. EXCEPT TO THE EXTENT SUCH A LIMITATION IS PROHIBITED BY LAW, IN NO EVENT WILL ANY PARTY'S TOTAL LIABILITY FOR ANY AND ALL DAMAGES AND CLAIMS UNDER OR RELATED TO THIS AGREEMENT EXCEED [ONE (1) CANADIAN DOLLAR].

Nothing in this Agreement will limit or exclude a Party's liability for death or personal injury caused by its negligence or for fraudulent misrepresentation or for any other liability which by law cannot be excluded.

7.0 TERM AND TERMINATION

7.1 **Term.** This Agreement commences as of the Effective Date and will continue until all Intellectual Property rights in or Confidentiality obligations relating to the Contributed Cyber Intelligence & Methods and Cyber Intelligence Repository have expired. This term of this Agreement for any particular Party will end upon the date of written notice to the CI-SOC Operator from the Party that it has elected to withdraw from the ("**Resignation Date**").

7.2 **Termination.** The CI-SOC Operator will have the sole right to terminate this Agreement in respect of any one or more breaching Parties by giving written notice: (i) if a Party has committed a material breach of any of its obligations under this Agreement, or an event occurs that otherwise expressly entitles the CI-SOC Operator to terminate this Agreement, which breach or event as not been remedied within a period of thirty (30) days following receipt of written notice to do so, (ii) if any circumstances arise which would entitle the court or a creditor to appoint a receiver, administrative receiver or administrator or to present a winding-up petition or make a winding-up order for a Party, (iii) if a Party makes any voluntary arrangement with its creditors for the general settlement of its debts or becomes subject to an administration order, or (iv) if a Party has an order made against it, or passes a resolution, for its winding-up (except for the purposes of amalgamation or reconstruction) or has a receiver or similar officer appointed over all or substantially all of its property or assets.

7.3 **Implication of Termination.** If a Party's rights under this Agreement end pursuant to Section 7.1 (Term) or terminate pursuant to Section 7.2 (Termination), all of the Party's license rights and entitlements relating to new instances of other Member's Contributed Cyber Intelligence & Methods and to ongoing access to or use of the Cyber Intelligence Repository will immediately end. However, the resigning or terminated Party's rights and obligations under this Agreement relating to other Members' Contributed Cyber Intelligence & Methods and the Cyber Intelligence Repository that arose prior to the date of resignation or termination will continue and survive, as will all pre-resignation or pre-termination license rights under this Agreement to their Contributed Cyber Intelligence & Methods. The provisions of this Agreement that are expressed or by their sense and context are intended to survive the termination of this Agreement will survive, including Sections 1 (Definitions), 2.6

(Subcontracting), 3 (Intellectual Property), 4 (Cyber Intelligence Security), 4.2 (Security), 5.2 (Warranty Disclaimer), 6 (Limitation of Liability), 7 (Term and Termination) and 8 (General) will survive termination.

8.0 GENERAL

8.1 **Notice.** All notices or reports required or permitted under this Agreement will be in writing and will be delivered by personal delivery, facsimile transmission, a nationally recognized overnight delivery service, by certified or registered mail, return receipt requested, or by electronic mail to be confirmed in writing delivered by one of the methods described herein, and will be deemed given upon personal delivery, electronic confirmation of electronic mail or facsimile transmission, or signature evidencing receipt of overnight delivery or registered mail, as applicable. Notices and communications between the Parties will be in English sent to the addresses of the Parties as shown in the Parties signature section or to such other addresses as each Party concerned may subsequently provide in writing to the other Parties.

8.2 **Additional Parties; Independence of Parties.** The Parties acknowledge that additional Parties may participate in the CI-SOC . In that event, the Parties agree that the additional Parties will execute this Agreement. All Parties will be informed of any additional Parties. None of the Parties will act or have the authority to act as an agent of any other Party for any purpose whatsoever. Nothing in this Agreement will be construed as forming a partnership, a joint venture or any other business relationship among the Parties.

8.3 **Assignment.** This Agreement will be binding on the Parties and their successors and permitted assigns. No Party will assign or otherwise transfer this Agreement or any of its rights and obligations whether in whole or in part without the prior written consent of the other Parties, which will not be unreasonably withheld. Any attempted assignment without such consent will be deemed a material breach giving the CI-SOC Operator the right to terminate this Agreement pursuant to Section 7.2(i). An assignment will be deemed to include: (i) any transaction or series of transactions whereby a third party acquires, directly or indirectly, the power to control the management and policies of the Party, whether through the acquisition of voting securities, by contract or otherwise: or (ii) the sale of more than fifty percent (50%) of the Party's assets whether in a single transaction or series of transactions. A mere change in a Party's organizational structure (such as reincorporation in a different jurisdiction or a change in legal form) not accompanied by a sale or other transfer of securities or assets, merger, reorganization, business combination or other similar transaction involving a third party will not be deemed a prohibited assignment or transfer under this Agreement. A Party may assign this Agreement without the other Parties' consent in connection with any merger, consolidation, reorganization, sale or other transfer of all or substantially all the business or assets of an operating group. CyberNB Inc.may assign its rights and obligations under this Agreement to a not-for-profit successor to CyberNB, to any alternate to CyberNB Inc.appointed by the Attorney General of New Brunswick to take over the leadership of the CI-SOC , or to a separate entity that is established to assume the ongoing responsibilities of the CI-SOC (in which case CyberNB Inc.will be deemed to be a Member and Party for the purpose of any remaining term of this Agreement).

8.4 **Applicable Law and Dispute Resolution.** This Agreement will be governed by, construed and interpreted in accordance with the laws of the Province of New Brunswick and the federal laws of Canada applicable therein, without regard to its conflict of laws provisions. The Parties will exert reasonable efforts to promptly arrive at an amicable settlement of any dispute which may arise between them out of or in connection with the Agreement. If, however, no such settlement is reached, then the Parties consent to the exclusive jurisdiction of the courts of New Brunswick for any dispute arising out of this Agreement.

8.5 **Severance.** If any provision of this Agreement is held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions will not in any way be affected or impaired, and such provision will be deemed to be restated to reflect the original intention of the Parties as nearly as possible in accordance with applicable law.

8.6 **Waiver.** The failure or delay of a party at any time or times to require performance by the other Party of any provision hereof, or to otherwise enforce any right or provision hereof, will not be deemed a waiver and will in no manner affect its right at a later time to enforce the same. Waiver of any breach or violation of this Agreement will not constitute a waiver of subsequent breach or violation of the same or different kind.

8.7 **Interpretation; Counterparts.** Unless otherwise expressly stated, when used in this Agreement "include," "includes," and "including" are not exclusive or limiting; and "Section" and "Subsection" refers to this Agreement's provisions. Section headings in this Agreement are for ease of reference only. The Parties may execute this Agreement in counterparts, which taken together will constitute one instrument.

8.8 **Entire Agreement.** This Agreement, including Schedules A and B, sets forth the entire understanding of each of the Parties with respect to the subject matter of this Agreement and supersedes any previous or contemporaneous agreements,

understandings or communications, whether written or oral, relating to such subject matter. This Agreement may be modified only by a written instrument executed by each the Parties.

8.9 **Anti-corruption.** Each of the Parties confirm their mutual anti-corruption commitment to each other that, in their business relationship, the Parties and their employees, agents and affiliates:

(i) will not give or receive any benefit which can be construed as an unlawful inducement to improperly benefit its business activities; and

(ii) will comply with all applicable anti-corruption laws in conducting its business.

In witness whereof the Parties have caused this Agreement to be executed by their duly authorized representatives as set forth below.

CyberNB

Party (Full Corporate Name): CyberNB Association Inc.

Signature: _____

Title: _____

Date: _____

I am authorized to sign on behalf of the Party named.

[MEMBER NAME]

Party (Full Corporate Name): _____

Signature: _____

Title: _____

Date: _____

I am authorized to sign on behalf of the Party named above.