PROTECTION OF PERSONAL INFORMATION AND CYBERSECURITY RULES
(LEGAL SERVICES/EXTERNAL COUNSEL)

(a) **Definitions**

"**Company Data**" means Company's Confidential Information, Personal Information and any other Company data in the Firm's or External Counsel's possession.

"**Confidential Information**" means information in whatever form, including verbal, written, and electronic information, data, programs, processes, accounts, specifications and reports, that is disclosed by the Company or its representatives to the Firm or External Counsel relating to (a) this Agreement, a PO, and/or a SOW, or (b) the Company's business and affairs, and includes all derivative information, reports, interpretations, and analyses generated from items (a) and (b). Confidential Information does not include information that is: (i) lawfully known to the Firm or External Counsel on a non-confidential basis prior to its receipt from the Company; (ii) generally known to the public, other than as the result of an act of the Firm or External Counsel or any third party under an obligation of confidentiality with regard to such information; or (iii) lawfully received by the Firm or External Counsel from a third party not bound to maintain such information as confidential.

"**Personal Information**" shall have the meaning provided under Law respecting the protection and privacy of Personal Information and, at a minimum, shall include any information about identifiable individuals provided to the Firm or External Counsel by Company for the Firm's or External Counsel's use in the performance of the legal services.

"**Process**" or "**Processing**" means any operation or set of operations performed upon any Company Data, whether or not by automated means, such as collection, recording, organization, structuring, adaption or alteration, retrieval, consultation, accessing, obtaining, storing, transmitting, using, maintaining, disclosing, or disposing of or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Security Incident**" means any actual or reasonably suspected: (i) accidental or unlawful destruction, loss, alteration, unauthorized disclosure, acquisition of or access to, theft, or other unauthorized Processing of Company Data transmitted, stored or otherwise Processed by the Firm or External Counsel; or (ii) unauthorized access to or use of, inability to access, or malicious infection of information systems that reasonably may compromise the confidentiality, availability or integrity of Company Data. For additional certainty, and for privacy law purposes, a Security Incident shall also include any unauthorized collection, access, use, or disclosure of Personal Information.

(b) **Confidentiality of Company Data.** The Firm and External Counsel acknowledges that under this Agreement, it may be provided with and have access to, and deemed to be in custody or control of, Company Data. The Firm and External Counsel agrees that it will only collect, use, disclose and retain Company Data for the purposes of performing the Work. The Firm and External Counsel also agrees to comply with Laws regarding Company Data and will safeguard Company Data. Without limiting the generality of the provisions of this Agreement relating to Confidential Information, the Firm or External Counsel acknowledges that (i) as and between the Firm/External Counsel and

Company, Company is the owner of any and all Company Data, and (ii) the Firm and External Counsel has no ownership rights or interest in any Company Data. The Firm and External Counsel shall not authorize a Subcontractor to process Company Data without the prior written consent of Company. References in this Article to the Firm and External Counsel shall include any affiliates, representatives or Subcontractors of the Firm or External Counsel, and the Firm and External Counsel shall remain liable for all actions of such affiliates, representatives or Subcontractors in respect thereof.

(c) **Privacy Notice to Individuals.** The Firm and External Counsel shall inform affected individuals of its Personal Information processing, protection, storing, and transferring practices by posting a notice (the "**Privacy Notice**") to such individuals on the information technology tools that affected individuals access or by other effective means of communicating the Privacy Notice, and contacting affected individuals with updates to the Privacy Notice whenever the Firm and External Counsel makes a material change to its Personal Information processing. The Company shall cooperate with the Firm and External Counsel in circulating the Privacy Notice to the affected individuals.

(d) **Security Controls and Information Management**. The Firm and External Counsel shall take appropriate administrative, physical, technical and organizational measures to ensure the confidentiality, integrity, availability and resilience of systems used for Processing Company Data and protect against the unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or use of Company Data transmitted, stored or otherwise Processed. Without limiting the generality of the foregoing, the Firm and External Counsel shall comply with the requirements set out by Law and industry standards and best practices relating to confidentiality, integrity, availability and security of Company Data, including standards and best practices of the Firm's and External Counsel's and Company's industry.

(i) The Firm shall implement access control systems, including identification and authentication mechanisms, on Firm's information systems that:

a. Controls to revoke access after several consecutive failed login attempts. Controls on the number of invalid login requests before locking out a user.
b. The ability to restrict access to the services to specific time periods and certain IP address ranges.
c. Where using passwords, protect passwords by, amongst other steps: establishing a procedure of disclosure, distribution and storage of passwords guaranteeing their confidentiality and integrity; ensuring that passwords are changed in accordance with the frequency set in the security document.
d. Unique user identifiers (user IDs), paired with passwords, to ensure that activities can be attributed to the responsible individual.
e. Apply best industry practice authentication mechanisms for any remote access provided or controlled by Firm to Company Data (e.g., VPN access).

(ii) The Firm and External Counsel shall ensure that its personnel engaged in Processing of Company Data are informed of the confidential nature of Company Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements in respect of Company Data that survive termination of the personnel engagement.

(iii) The Firm shall maintain physical access controls, secure user authentication protocols, secure access control methods, firewall protection, and intrusion detection and prevention mechanisms.

(iv) The Firm, or an authorized third party, shall 24/7 monitor the Firm's systems and/or the Firm's Processing of Company Data for unauthorized intrusions using network-based intrusion detection mechanisms.

(v) The Firm shall implement up-to-date firewalls between the Firm's systems, the Internet (including internal networks connected to the Internet) and other public networks, and internal networks that are not necessary for processing Company Data; the firewalls must be reasonably designed to maintain the security of Company Data and relevant information systems.

(vi) The Firm shall maintain an inventory in a way that provides traceability to those media, servers, and equipment containing Company Data.

(vii) The Firm shall maintain controls in accordance with Industry Standards, including encryption where appropriate, to protect Company Data and communications during transmissions between Company's network and the Firm and/or External Counsel.

(viii) The Firm shall ensure that all Company Data is stored and backed up in a manner consistent with Industry Standards and at a reasonable frequency.

(ix) The Firm shall implement and maintain any additional security safeguards, as directed by Company, in the event of any (i) material changes to any Work, or any relevant technology or systems; (ii) information Security Incident; or (iii) the discovery of a material security vulnerability or weakness, as determined by Company in its sole discretion.

(x) The Firm shall provide Company log entry records to assist in forensic analysis if there is suspicion of inappropriate access.

(xi) The Firm shall, consistent with applicable Law and Industry Standards, collect and record information, and maintain logs, planning documents, audit trails, Records and reports, concerning: (i) the Firm's and/or External Counsel's Processing of Company Data; and (ii) information Security Incidents.

"**Industry Standards**" means industry standards and best practices relating to the confidentiality, integrity, availability or security of Company Data, including, without limitation, standards and best practices of Contractor's industry, [including NIST CSF; NIST SP 800-53; NIST SP 800-37; ISO 27001/27002; CISA guidelines and best practices]

(e) **Notice of Transfer of Company Data.** The Firm and/or External Counsel shall provide Company with advance written notice if the Firm and/or External Counsel intends to transfer or permit access to, Company Data outside of Canada or the United States for the purposes of performing the Work. In the event of such transfer or access of Company Data, the Firm shall remain responsible and liable for the protection of such Company Data, including implementing security measures for its protection and compliance with all Laws.

(f) **Access, Correction and Deletion Requests.** The Firm and/or External Counsel shall notify Company as soon as reasonably possible of any access, correction or deletion requests of Personal Information, and will work with Company to respond accordingly.

(g) **Destruction of Personal Information.** Upon termination of this Agreement, or upon written request by Company, the Firm shall promptly return all Personal Information in a form accessible

and readable by Company and, to the extent technologically and financially feasible, after returning Personal Information to Company, Firm shall delete Personal Information from their systems and databases no later than thirty (30) calendar days from the date this Agreement terminates, or earlier upon written request from Company. If requested by Company, Firm shall also provide a Certificate of Destruction duly executed by an authorized signatory within thirty (30) calendar days of such request. Upon termination of this Agreement, Firm shall have no further entitlement or access to Personal Information for any purpose whatsoever, unless required by Law or otherwise expressly authorized by Company.

(h) **Security Incident Notification.**

(i) The Firm shall, within twenty-four (24) hours of a suspected or actual Security Incident, provide notice to Company by contacting Company at email (cyber.escalations@southbow.com). In its notification, the Firm shall provide the following:

a. full details of the Security Incident;
b. full details of Company Data compromised, including the categories and approximate number of Company Data records concerned, including Personal Information;
c. where known, details of the likely consequences of the Security Incident;
d. full details of how the Security Incident is being investigated and mitigation and remedial steps already put in place and to be put in place.

(ii) The Firm shall take all necessary steps, at the Firm's cost and expense, to investigate, correct and mitigate the Security Incident and shall comply with all applicable reporting obligations required by applicable Law. In the event the Firm experiences a Security Incident, the Firm shall fully reimburse Company for any resultant fines, penalties, or other remedies assessed against Company by any applicable governmental authority or regulator, plus any cost(s) associated with related notifications, investigations, enforcement, credit monitoring and/or identity protection services provided to the individuals affected by the Security Incident for two (2) years following the date Company deems the Security Incident to have occurred. For greater certainty, the costs and expenses relating to such notices, investigations, enforcement, monitoring, fines and/or penalties shall be separate and apart from any general limitation on liability otherwise contained in this Agreement.