fundserv

Data Protection Schedule

This Schedule applies to the collection, use, disclosure, storage, and any other types of processing (collectively "**processing**") of personal information transferred by Customer to Fundserv for processing on behalf of Customer ("**Customer Personal Information**") in order to perform services ("**Services**") to Customer pursuant to the agreement, referred to as the "Customer Contract", between the parties ("**Agreement**").

The parties agree as follows:

1. Compliance with Data Protection Laws. Each of Customer and Fundserv shall comply with applicable Canadian federal and provincial laws, orders and regulations governing the processing of personal information, including the *Personal Information Protection and Electronic Documents Act* and substantially similar provincial laws ("**Data Protection Laws**"), and will provide reasonable cooperation to each other to the extent such cooperation is necessary for each party's compliance with Data Protection Laws.
2. Purpose limitation; ownership. Any processing of Customer Personal Information by Fundserv shall be limited to what is necessary to provide the Services or such other purposes authorized by the Customer or required or permitted under applicable Data Protection Laws. Customer Personal Information shall at all times be and remain the sole property of the Customer.
3. Consent. Customer represents and warrants that, to the extent required by applicable law, it has obtained appropriate consent from individuals to whom personal information relates as necessary for Fundserv to process information required to provide the Services contemplated by the parties under this Schedule and the Current Member Contract. The parties acknowledge and agree that the above consent may not be required in respect of certain processing where required or permitted in accordance with Data Protection Laws.
4. Compliance. Client shall maintain controls to ensure Local Registration Authorities and end-users comply with all requirements reasonably imposed by Fundserv to safeguard the confidentiality and security of Customer Personal Information and Fundserv systems, including those set out in Fundserv's Privacy Policy, the LRA Guide and any Fundserv communications. Further, Client shall restrict access to end-users who need such access to perform their duties and shall immediately notify Fundserv of any unauthorized access to Customer Personal Information or information relating to other Fundserv clients.
5. Sub-processors. Customer authorizes Fundserv to appoint sub-processors to process Customer Personal Information on its behalf. Fundserv shall ensure that the arrangement between Fundserv and the sub-processor is governed by a written contract which offers at least the same level of protection for Customer Personal Information as those set out in this Schedule.
6. Cross-border Transfers. Fundserv may only process, and shall ensure that its sub-processors only process, Customer Personal Information in Canada, and the United States, unless Fundserv provides reasonable prior notice to Customer.
7. Data Subjects' Requests under Data Protection Laws. If Fundserv receives an individual's request regarding the Customer Personal Information under Data Protection Laws, Fundserv shall promptly redirect such request to Customer, and agrees to reasonable cooperation with Customer to respond to such request in accordance with Data Protection Laws.
8. Data Security Program. Fundserv shall maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to the need for security and confidentiality of such information as set out in Schedule A ("**Security Program**"). Fundserv's Security

Program shall be designed to: (a) protect the confidentiality, integrity, and availability of the Customer Personal Information in Fundserv's possession or control or to which Fundserv has access; (b) protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Customer Personal Information; (c) protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of the Customer Personal Information; (d) protect against accidental loss or destruction of, or damage to, Customer Personal Information; and (e) safeguard Customer Personal Information in accordance with Data Protection Laws.

9. Data Incidents

9.1. **Informing Customer of Data Incident.** Fundserv shall without delay notify Customer of any loss of, or unauthorised access to or use or disclosure of, Customer Personal Information or any other breach or attempted breach, by any person, of Fundserv's Security Program or otherwise in the protection of Customer Personal Information ("**Data Incident**"). Fundserv shall promptly take all reasonably necessary corrective actions to mitigate the adverse effects of Data Incident. Customer shall be responsible for applicable notification and/or reporting requirements under Data Protection Laws. Fundserv shall provide reasonable cooperation to Customer in respect of applicable notification and/or reporting requirements under Data Protection Laws.

10. Security Review and Verification

10.1. At Customer's reasonable request and in satisfaction of the Customer's need to undertake a verification relating to confidentiality requirements, Fundserv will provide Customer copies of (i) its data protection, privacy and security policies and procedures that apply to the Customer Personal Information, and (ii) Fundserv's third party assurance dealing with, inter alia, privacy, security, and integrity of data. Customer shall treat all such information disclosed by Fundserv as Confidential Information as defined in the Agreement.

11. User Acceptance Testing Environment

11.1. Fundserv makes available a User Acceptance Testing (UAT) environment to facilitate training new Customers on its systems and to give existing Customers the opportunity to test new functions prior to the functions entering production. Customer may only upload data to the UAT environment that does not contain Customer Personal Information. Any data uploaded to the UAT environment is not subject to the protections of this Schedule.

12. Interpretation and Secure Disposition

12.1. This Schedule shall, upon execution by the parties, become an integral part of the Agreement and constitute, with the Agreement, the entire agreement between the parties with respect to the subject matter thereof, and any prior representations, statements, and agreements relating thereto are superseded by the terms of the Agreement. For clarity, the exclusion of liability under the Agreement shall be deemed to be consistent with the provisions of this Schedule and shall exclude all Fundserv liability for breach of any provision of the Schedule.

12.2. Fundserv shall either securely return or dispose of all Customer Personal Information in its possession or in the possession of any third party to whom it transferred Customer Personal Information within a reasonable period following expiry or termination of the Agreement in accordance with Fundserv's standard retention schedule unless retention of such transferred personal information is permitted or required by Applicable Laws.

Appendix A

Security Program Minium Requirements

Fundserv's Security Program includes the following:

a) **Security Awareness and Training.** A mandatory security awareness and training program for all members of Fundserv's workforce (including management), which includes: (i) training on how to implement and comply with its Security Program; and (ii) promoting a culture of security awareness through periodic communications from senior management with employees.

b) **Background Assessment and Monitoring.** Policies and procedures to conduct appropriate assessments for all current and prospective members of Fundserv's workforce who have access to Customer Personal Information.

c) **Access Controls.** Policies, procedures, and logical controls: (i) to limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons with a genuine need-to-know; (ii) to limit the amount of Customer Personal Information is made accessible to authorized persons as required to carry out their job-related functions; (iii) to limit access to those workforce members and others who should not have access from obtaining access; and (iv) to remove access in a timely basis in the event of a change in job responsibilities or job status or as a result of a failed background assessment. As part of its suite of access controls, Fundserv delegates the role of Local Registration Authority (LRA) to an individual at each organization. Each LRA has certain responsibilities, including providing end users with access to Fundserv's environment. For more information about an LRA's roles and responsibilities, please consult your Access Manager LRA Guide.

d) **Physical and Environmental Security.** Controls that provide reasonable assurance that physical access to facilities where Customer Personal Information is stored, including physical servers, is limited to properly authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include: (i) logging and monitoring of unauthorized access attempts to Fundserv's facilities by security personnel; (ii) camera surveillance systems at critical internal and external entry points of Fundserv's facilities; (iii) systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and (d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

e) **Data Incident Procedures.** A data incident response plan that includes procedures to be followed in the event of any actual or reasonably suspected Data Incident. Such procedures include: (i) formation of an internal incident response team with a response leader; (ii) assessing the risk the incident poses and determining who may be affected; (iii) internal reporting; (iv) keeping a record of what was done and by whom to help in later analysis and possible legal action; and (v) conducting and documenting root cause analysis and remediation plan.

f) **Contingency Planning.** Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic, and natural disaster) that could damage Customer Personal Information or production systems that contain Customer Personal Information. Such procedures include: (i) a policy for performing periodic backups of production file systems and databases containing Customer Personal Information, according to a defined schedule; (ii) a formal disaster recovery plan for Fundserv's facilities where Customer Personal Information is stored; and (iii) a formal process to

address the framework by which an unplanned event might be managed to minimize the loss of vital resources.

g) **Audit Controls.** Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information. Such mechanisms must ensure that actions are attributable to an identifiable individual.

h) **Data Integrity.** Policies and procedures to safeguard the confidentiality, integrity, and availability of Customer Personal Information and protect it from disclosure, improper alteration, or destruction.

i) **Storage and Transmission Security.** Security measures to guard against unauthorized access to Customer Personal Information that is being transmitted over a public electronic communications network or stored electronically. Such measures include (i) limiting the use of portable storage devices, such as USB (Universal Serial Bus) drives, to store or transfer Customer Personal Information to the extent demonstrably necessary to fulfill a specific purpose; and (ii) encryption during transmission.

j) **Segmentation.** Measures ensuring the segmentation of Customer Personal Information from data of others.

k) **Assigned Security Responsibility.** Assigning responsibility for the development, implementation, and maintenance of its Security Program, including: (i) designating a security official with overall responsibility; and (ii) defining security roles and responsibilities for individuals with security responsibilities.

l) **Testing.** Periodically testing the key controls, systems, and procedures of its Security Program to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing shall be conducted by qualified independent third parties.

m) **Logging and Monitoring.** Network and systems monitoring, including error logs on servers, disks, and security events for any potential problems. Such monitoring includes: (i) reviewing material changes affecting systems handling authentication, authorization, and auditing; (ii) reviewing privileged access to Fundserv's production systems; and (iii) engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

n) **Change and Configuration Management.** Maintaining policies and procedures for managing changes Fundserv makes to production systems, applications, and databases. Such policies and procedures must include: (i) a process for documenting, testing and approving the patching and maintenance of the Service; (ii) a security patching process that requires patching systems in a timely manner based on a risk analysis; and (iii) a process for Fundserv to utilize a third party to conduct web application-level security assessments.

o) **Program Adjustments.** Fundserv will monitor, evaluate, and may adjust, as appropriate, the Security Program in light of: (i) any relevant changes in technology and any internal or external threats to Fundserv or the Customer Personal Information; (ii) security and data privacy regulations applicable to Customer and/or Fundserv; and (iii) Fundserv's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

p) **Devices.** All laptop and desktop computing devices utilized by Fundserv and any subcontractors when accessing Customer Personal Information must: (i) be equipped with encryption; and (ii) employ reasonable security safeguards to protect such devices in accordance with industry standards.