SECURITY REQUIREMENTS FOR DATA LICENSEES

Overview of these Requirements

1. This page sets out specific measures the Licensee must take under its Agreement in order to protect the Data, including in a bulk, raw, and/or manipulable format (as described in the definition of "Licensed Data" below) and the Data irrespective of the format or amount.

Definitions in these Requirements

2. Terms capitalized but not defined in these requirements have the meaning provided in the Agreement. In these requirements:

   (a) "**Agreement**" means the license agreement between BCA and the Licensee.

   (b) "**Authorized Personnel**" means directors, officers, employees, agents and contractors of the Licensee authorized to access the Data for purposes of the Agreement.

   (c) "**BCA**" means the British Columbia Assessment Authority.

   (d) "**Data**" means the data BCA provides to the Licensee in respect of Folios located within British Columbia under the Agreement.

   (e) "**Licensed Data**" means the Data, except where the Data is: (a) provided in a Value Added Product that complies with the Agreement, including that the Licensee is not providing the Value Added Product in any way that would enable a third party to extract or copy the lesser of 300 Folios and the maximum number of Folios permitted under Schedule B, at a time; or (b) the Data has been transformed into a state where a third party would not be able to extract or copy 300 or more Folios (or data from 300 or more Folios).

   (f) "**Licensee**" means the person who licenses Data from BCA.

   (g) "**Transportable Media**" means all types of transportable storage media on which data can be saved, including, but not limited to, laptops, CD-ROMs, flash memory sticks and removable hard disks.

Security Requirements

3. The Licensee shall communicate the requirements set out in these requirements to Authorized Personnel prior to them accessing the Data.

Physical Access

4. The Licensee shall only store and access the Licensed Data in a location to which access is controlled on a 24/7 basis.

5. The Licensee shall restrict access to the Licensed Data to Authorized Personnel.

Storage and Transmission

6. All computers and other devices with access to the Licensed Data must employ logical access controls (passwords) at the device and network level.

7. Where the Licensed Data is held on Transportable Media, passwords and full encryption must be used. This applies equally to backups of the Data stored on Transportable Media. The Licensee may transport the Licensed Data on Transportable Media, provided the Licensed Data is in transport for as little time as reasonably possible and the transportation otherwise complies with the Agreement (including these requirements).

8. The Licensed Data cannot be electronically transmitted, except as described in points 6 and 7. Electronic transmission includes transmittal of the Data by web browser or by email.

9. Servers storing and transmitting the Licensed Data must be located in a secure, controlled-access area, preferably in the same area where the Licensed Data is accessed. If located in a separate area, controls must be in place to ensure that only Authorized Personnel can access the servers.

10. Network firewalls and access rules must be in place to prevent unauthorized access to the Licensed Data. Licensed Data may be stored on and transmitted over networks not meeting these requirements, provided that it is encrypted (except when in use by Authorized Personnel). Alternatively, the Licensed Data may be stored on a stand-alone computer with no external connections, or on a closed network (for greater certainty, the Data must be encrypted while it is stored on any stand-alone computer). When a network transmits Licensed Data that leaves a secure area (for example, when the Authorized Persons are housed in a series of buildings), the Licensed Data must be encrypted whenever it is outside the secure area.

11. Notwithstanding anything else in these requirements, the Licensed Data must be encrypted at all times, both inside and outside the secure area and both in transport or at rest (in storage).

12. Where the Licensed Data is available to the public, or a subset of the public or any other third party as part of a Value Added Product, the Licensee shall take steps to prevent third parties, including End Users, from accessing, copying or using the Licensed Data in violation of the Agreement (such as by extracting or copying 300 or more Folios). For example, the Licensee shall maintain security measures to prevent the Data from being copied or extracted through web scraping or harvesting.

Physical Storage

13. When not in use, Transportable Media containing the Licensed Data must be stored in secure containers. This applies equally to backups of the Licensed Data.

14. When not in use, printed documents containing the Licensed Data must always be stored in secure containers.

Data Copying and Retention & Record Management

15. Copies and extracts of the Licensed Data may only be made for the purposes permitted by the Agreement. When no longer needed, any such copies or extracts must be destroyed in a secure manner (as per points 16 and 17 below).

16. Paper documents containing the Licensed Data must be destroyed (shredded) in a secure manner before disposal. Any destruction must occur within the secure area.

17. All electronic storage media used in the processing of the Licensed Data, including all backups, Transportable Media, photocopiers and other electronic media where the Licensed Data has been electronically stored will be sanitized or destroyed when disposing of such media or when return or destruction of the Licensed Data is required by BCA or pursuant to the Agreement. Any destruction must occur within the secure area.