INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÉRES

May 27, 2011

Mr. Jacques Tanguay
Vice-President, Regulatory Division
Bourse de Montréal Inc. (the Bourse)
Tour de la Bourse, P.O. Box 61
800 Victoria Square I
Montreal, Quebec H4Z 1A9

Dear Mr. Tanguay:

Re: Confidentiality Agreement re Large Open Position Reporting (LOPR)

Please find attached a draft Confidentiality Agreement as discussed on May 3rd and referred to in our last correspondence dated May 20, 2011. As you will note from the draft, the Confidentiality Agreement is to be agreed to and signed by the Bourse and Approved Participants (APs).

We would appreciate receiving any proposed changes and ultimately sign-off on this important document given the quantity of personal information that Approved Persons are required to provide to the Bourse under the LOPR initiative. The amount of information is significantly more than what is required to be provided to other regulators or government bodies on a daily basis and the agreement is consistent therefore with the level of information security expected.

As noted in our May 20, 2011 letter, the issues surrounding privacy of personal information mean that until the required Rule changes are in place and the confidentiality agreement is executed, most if not all APs will be unable to provide personal information (as defined in the Personal Information Protection and Electronic Documents Act) using either the SAIL LOPR protocol or the LOPR GUI during the production deployment period that was to have started May 2, 2011.

We look forward to hearing from you regarding the agreement as soon as you are able.

Yours truly,

"Original singed by Deb Wise"

Deborah Wise
Assistant Director
dwise@iiac.ca; (416) 687-5472

"Original signed by Barb Amsden"

Barbara Amsden
Director
bamsden@iiac.ca; (416) 687-5488

Cc : Anthony Tamvakologos; François Gilbert

Attachment

BOURSE DE MONTRÉAL INC./APPROVED PARTICIPANT

LOPR CONFIDENTIALITY/NON-DISCLOSURE/SECURITY AGREEMENT

This Confidentiality/Non-Disclosure/Security Agreement (this "Agreement") is made as of the ___th day of _____, 20__ between:

- The **Bourse de Montréal Inc., also known as the Montréal Exchange Inc.** (the Bourse), with offices located at 800, rue du Square-Victoria, Montreal, QC H4Z 1A1 *[Note: Bourse to confirm legal names, address]*

AND

- **__Name___** , a Bourse Approved Participant (AP) that is required to provide Confidential Information to the Bourse to meet Large Open Position Reporting (LOPR) requirements.

RECITALS:

Whereas: the Bourse requires Approved Participants to provide the Bourse with Confidential Information to meet LOPR requirements under Rule 14, Article 14102 in order to automate as well as increase confidentiality and security of information used for regulatory purposes of supervision, enforcement and discipline to ensure the fair and efficient operation of exchange-based derivatives markets in Canada *[Note: Bourse to confirm regulatory purpose]*;

Whereas: the AP requires that any company or individual to which or to whom, respectively, it discloses Confidential Information to enter into a legal agreement to implement and/or meet appropriately rigorous Information Security Protection Requirements to ensure the confidentiality and security of, and prevent the unauthorized use and disclosure of, the Confidential Information;

Whereas: the Bourse and the AP (the Parties) wish to set out the terms under which the AP will disclose Confidential Information to the Bourse and upon which the Bourse is willing and obliged to keep such information of the AP confidential;

NOW THEREFORE, in consideration of good and valuable consideration the receipt and sufficiency of which is irrevocably acknowledged by the Parties, the Parties agree to the following:

1. Definitions

"Approved Participant" or "AP" means an approved participant (including a foreign Approved Participant) of the Bourse, whose name is duly recorded as such on the register

referred to in article 3010 of the Rules of the Bourse and who is approved by the Bourse pursuant to its Rules for the purposes of trading products listed on the Bourse

"Bourse" means the Bourse de Montréal Inc., also known as the Montréal Exchange Inc., and including the Regulatory Division of the Bourse de Montréal Inc.

"Bourse Representative" means those employees, affiliates, agents, advisors, consultants, contractors, subcontractors and other third-party representatives engaged by the Bourse for the purposes of analysing the LOPR

"Confidential Information" refers to:

- client Personal Information that the Bourse requires be included in Large Open Position Reporting;
- proprietary AP information;
- any other information provided to the Bourse under the LOPR requirements or through LOPR reporting systems; and
- information that by the nature of the circumstances surrounding the disclosure or receipt, or by the nature of the information itself, would be treated as proprietary and confidential by a reasonable person

"Information Security Requirements" means information security protections that reflect best financial industry practices including:

(i) an information security governance framework

(ii) a written and comprehensive set of information security policy documents that act as the rules and guidelines for dealing with the Confidential Information with appropriate administrative, technical and physical safeguards to ensure the safety and confidentiality of Confidential Information, including when the Bourse's business continuity and disaster recovery plans are required to be implemented

(iii) technological, physical, organizational and other security safeguards itemized in Appendix 1 to protect Confidential Information in transit and in storage against anticipated threats or hazards, loss, theft, unauthorized access, disclosure, copying, use, modification, disposal and destruction, including an appropriate level of cryptographic integrity and strength that is greater than or equal to that of the originally supplied Confidential Information provided electronically

(iv) quarterly intrusion testing of the Bourse's physical, logical and information security controls

(v) no less frequent than annual reviews of the Bourse's existing information security processes and procedures by external auditors with appropriate expertise to conduct a Canadian Institute of Chartered Accountants (CICA) 5970 audit or an equivalent SAS 70 Type II audit as determined by the American Institute of Certified Public Accountants (AICPA)

(vi) no less frequent than annual reviews of information security best practices and upgrades to any aspects of information security found to be inconsistent with best practices

"Large Open Position Reporting" or "LOPR" means reporting required by the Regulatory Division of the Bourse of long and short positions in options and futures under Rule 14, Article 14102

"Party/Parties" means an Approved Participant and/or the Bourse

"Personal Information" means that required for LOPR and defined in Privacy Laws, including the following data elements:

- Client name
- Client address (including city, province, country and postal code)
- Client phone number, fax number, e-mail address
- Account number
- Social Insurance Number, or any part thereof
- Any other data elements specified in LOPR requirements

"Privacy Laws" means the Personal Information Protection and Electronic Documents Act (S.C.2000, c.5) (PIPEDA) and any successor legislation or the legislation of a province if the legislation is declared to be substantially similar to PIPEDA and any applicable regulations, as well as any other privacy law or regulation applicable to the Confidential Information

"Security Incident" means unauthorized access to, disclosure or loss of, or inability to account for, any Confidential Information of the AP

2. Ownership of Confidential Information

All Confidential Information is and will remain the exclusive property of the AP, and the Bourse will have no rights to the Confidential Information except as expressly provided for in the Agreement.

3. Access to Confidential Information by Bourse Representatives

The Bourse will not request Confidential Information beyond what is the minimum necessary to fulfill the purpose(s) for which it is requested and will ensure that:

(i) While in the possession of the Bourse, Confidential Information will be:
   a. subject to the oversight of a designated employee who is responsible for all Confidential Information in the Bourse's possession or under its control and for ensuring that the Bourse complies with the provisions of this Agreement;
   b. protected as required by, and in compliance with, all Privacy Laws, this Agreement, and the Information Security Requirements as of the date the Agreement is signed by the Bourse and continuously while the Confidential Information is in the possession of the Bourse; and
   c. stored, accessed, handled, used and disposed of only in Canada;

and that:

(ii) All Bourse Representatives:
   a. sign a non-disclosure agreement requiring the particular individual to keep confidential all Confidential Information to a level no less stringent than required by this Agreement;
   b. have an understanding of information risk management threats and concerns related to the Confidential Information; and

c. receive privacy compliance and security training and regular updates on relevant information risk management policies and procedures.

4. Use and Disclosure of Confidential Information by Bourse Representatives

The Bourse will handle Confidential Information received, collected or accessible to the Bourse in accordance with all Privacy Laws and will not:

(i) use Confidential Information of the AP for any purpose other than LOPR, as may be amended from time to time following due consultation with all APs;

(ii) disclose or provide access to any Confidential Information except as permitted by this Agreement; and

(iii) copy or reproduce the Confidential Information except as may be required for the performance of LOPR analysis and to otherwise not make copies or partial copies of the Confidential Information without, on reproduction, containing the same proprietary and confidential notices and legends to preserve the protected status of the Confidential Information.

5. Receipt and Storage of Confidential Information

The Bourse will keep the Confidential Information provided by the AP logically isolated from any other data of the Bourse or other third parties so that:

(i) AP Confidential Information is not commingled with third party data or disclosed in conjunction with any disclosure of other data;

(ii) the Bourse can readily locate and destroy Confidential Information in accordance with this Agreement; and

(iii) the Bourse can take appropriate steps to ensure Confidential Information is safeguarded:

a. in accordance with industry-accepted best practices and standards used or observed by comparable companies in North America; and

b. by adopting and complying with documented policies and procedures designed to protect against any anticipated threats or hazards to the security or integrity of Confidential Information, and against any loss, theft, unauthorized access, use, disclosure, copying, or modification.

6. Destruction of Confidential Information

The Bourse will promptly, by secure means, destroy so that it is physically or virtually irrecoverable all copies of AP Confidential Information in any format that is seven years past the date of receipt or no longer necessary to fulfill the purpose(s) for which it was made available so that the Confidential Information is not able to be used maliciously or fraudulently against the AP, its employees or customers. In carrying out any destruction, the Bourse will protect Confidential Information in accordance with the terms of this Agreement by shredding hardcopy or placing it in secure disposal boxes and by ensuring electronic data is destroyed to at least a "7x Overwrite" level.

7. Exceptions to Requirements

The provisions of Sections 3, 4 and 5 will not apply to any information that the Bourse can establish by documentary evidence:

(i) was already known by the Bourse at the time of initial disclosure by the AP;

(ii) is or becomes publicly known through no wrongful act of the Bourse or Bourse Representatives, or any other person subject to a confidentiality agreement in favour of the AP;
(iii) is rightfully received from a third party without similar restriction provided that the third party did not come into possession of the Confidential Information as a result, directly or indirectly, of a breach of an obligation of confidentiality owed by any person to the AP; or
(iv) can establish was independently developed by or on behalf of the Bourse without reference to the AP Confidential Information.

The foregoing does not apply in the case of Personal Information.

8. Compelled Disclosure.

The Bourse may disclose AP Confidential information if:
(i) the disclosure is approved by written authorization of the AP; or
(ii) the Bourse is legally obligated to disclose the AP Confidential Information whereupon the Bourse will:
   a. give the AP prompt written notice sufficient to allow the AP to seek a protective order or other appropriate remedy, and will reasonably co-operate with the AP's efforts to obtain such protective order or other remedy at the AP's expense and, in the event that the Bourse is unable to do so, will, as long as not prohibited by law, advise the AP immediately subsequent to such disclosure;
   b. disclose only such information as is required, in the opinion of the Bourse's counsel; and
   c. use commercially reasonable efforts to obtain confidential treatment for any Confidential Information that is so disclosed.

9. Unauthorized Disclosure of Confidential Information

If there is any Security Incident, the Bourse will promptly, and in any event no later than two business days after becoming aware thereof:
(i) notify the AP of the Security Incident through contact channels maintained by the Bourse;
(ii) take such actions as may be necessary or reasonably requested by the AP to minimize the disclosure or loss;
(iii) co-operate in all reasonable respects with the AP to minimize the impact and any damage resulting from the Security Incident; and
(iv) work with the AP to confirm the nature of the Security Incident and, if the AP determines that the Security Incident must be reported to AP clients or other third party, agree with the AP on the form and content of any notification to AP clients regarding the Security Incident.

10. Required Communications

The Vice-President of the Bourse will provide annually to the AP signed written confirmation with respect to the previous 12-month period that:
(i) to the best of the Bourse's knowledge, after reasonable inquiry, the Bourse has complied with the requirements set forth in this Agreement, with the exception of those incidents of non-compliance communicated to the AP in writing;

(ii) that all records older than seven years have been destroyed in accordance with the Agreement;
(iii) the Bourse's information security policy and privacy compliance processes have been reviewed and confirmed or updated;
(iv) the cover letter signed by a recognized auditor with the results of the CICA 5970 or SAS 70 (Type II) audit is attached; and
(v) a summary of changes that have been or are to be made to upgrade information, physical and logical security.

The Bourse will, unless prohibited from doing so by applicable law, refer to the AP all requests for access to Confidential Information, including by an AP client, and respond to any such request only by making reference to such referral; if AP is required by any applicable law to provide AP Confidential Information that is in the Bourse's possession or control to an individual, at AP's request, and provided that AP has provided the Bourse with reasonable prior notice, the Bourse will provide such Confidential Information and meet any deadlines for the Confidential Information's provision required to enable AP to comply with any deadlines under applicable law.

11. Right to Review Adherence to Agreement

The Bourse will permit an individual authorized and named in writing by the Investment Industry Association of Canada (IIAC), on behalf of IIAC AP members, to enter, during normal business hours and on prior written notice from time to time and no more frequently than annually (unless there is documentary or other reasonable evidence of disclosure by the Bourse of Confidential Information) any premises of the Bourse at which Confidential Information is stored or used and audit the procedures, processes and information pertaining to the Bourse's compliance with this Agreement.

12. No Warranty

No warranties of any kind are given by the AP with respect to the accuracy, appropriateness or completeness of information provided to the Bourse although the AP makes all reasonable efforts to ensure accuracy of Confidential Information. In particular, the AP assumes no liability at all for any data provided in unreconciled format.

13. Indemnity

The Bourse hereby covenants and agrees that it will indemnify and save the AP harmless from and against any and all liability, loss, damages, claims, costs and expenses (including without limitation legal fees) that the AP may at any time incur, suffer or be required to pay arising out of or in any way related to a breach of this Agreement by the Bourse or the Bourse Representatives.

14. Liability

The Bourse will be liable for any failure by Bourse Representatives to comply with the terms of this Agreement. Further to Section 12, the Bourse will be liable for any cause of action brought against an AP by an AP client due to data aggregated under the LOPR Requirements to link accounts that are inappropriate from a business relationship perspective or due to raw data provided that later on reconciliation proves to be incorrect.

15. Injunctive Relief

The Bourse acknowledges that disclosure or use of Confidential Information in violation of this Agreement could cause irreparable harm to the AP for which monetary damages may be difficult to ascertain or be an inadequate remedy. The Bourse therefore agrees that the AP will have the right, in addition to its other rights and remedies, to seek injunctive relief for any violation of this Agreement.

16. Limited Relationship

This Agreement will not create any relationship or obligation to form any relationship between the Parties. Each Party will act as an independent contractor and not as an agent of the other Party for any purpose, and neither will have the authority to bind the other.

17. Cumulative Obligations

Each Party's obligations hereunder are in addition to, and not exclusive of, any and all of its other obligations and duties to the other Party, whether express, implied, in fact or in law.

18. Entire Agreement

This Agreement constitutes the entire agreement between the Parties relating to the protection of the secrecy or confidentiality of the Confidential Information.

19. Amendment

This Agreement may be amended or modified only with the mutual written consent of both Parties.

20. General Terms

The Bourse's obligations under this Agreement are perpetual and the Bourse may not assign the obligations and benefits of this Agreement. This Agreement inures to the benefit of the AP and its successors and assigns and is binding upon the Bourse's successors. This Agreement is intended to apply to all Confidential Information that is disclosed by the AP to the Bourse or that is otherwise learned by or comes into the possession or knowledge of the Bourse, whether prior to, on or subsequent to the date hereof. Either party may terminate this Agreement by providing written notice to the other. Notwithstanding the termination of this Agreement, the obligations set out here will continue to apply with respect to Confidential Information disclosed prior to receipt of such written notice for as long as the exceptions in Section 7 do not apply to such information.

21. Non-waiver

Any failure by either Party to enforce the other Party's strict performance of any provision of this Agreement will not constitute a waiver of its right to subsequently enforce such provision or any other provision of this Agreement.

22. Governing Law

This Agreement will be governed by and construed in accordance with the laws in force in the Province of Ontario and the Parties attorn to the non-exclusive jurisdiction of the courts of Ontario. This Agreement may be executed in counterparts and each such counterpart will constitute an original document and such counterparts, taken together, will constitute one and the same instrument. Any provision of this Agreement that is prohibited or unenforceable in

any jurisdiction will, as to that jurisdiction, be ineffective to the extent of the prohibition or unenforceability without invalidating the remaining provisions and any such prohibition or unenforceability in any jurisdiction will not invalidate or render unenforceable such provision in any other jurisdiction.

23. Contacts

The following are the duly senior authorized contact particulars for the Bourse and the AP with respect to this Agreement**.**

For the Bourse, the contact is: *[Note: To be completed by the Bourse, including title, telephone number, e-mail address and fax number]*.

For the AP, the contact is: *[Note: To be completed by the AP, including title, telephone number, e-mail address and fax number]*

24. Notices

With the exception of Section 8, where communication should be by secure e-mail and phone, any notice, request, demand, consent or other communication required or permitted under this Agreement will be given by personal or couriered delivery, in writing, to the contact person nominated in Section 23 by the AP or the Bourse, as the case may be. Either Party may change the address or addressee for the purposes of receipt of communications by giving not less than ten (10) calendar days' prior written notice to the other Party in the manner set out in this section. Any notice so given is deemed to have been received on the second business day following the date it was delivered.

In witness whereof, the Parties have executed this Agreement on the date first written above and the undersigned are duly authorized to sign this Agreement.

Bourse de Montréal Inc.	**[Other Parties]**
By: _____	By: _____
Title: _____	Title: _____
Date: _____	Date: _____

Appendix 1

Information Security Protection Requirements Best Practices

1. Security Policy

The Bourse will have an information risk management policy that: (i) communicates management commitment and information security requirements to all levels of the organization; (ii) aligns with ISO 27002:2005; and (iii) has been approved and reviewed by management within the last twelve (12) months.

2. Asset Management

The Bourse will ensure all equipment will be controlled and monitored within an asset management system.

3. Physical and Environmental Security

The Bourse will:

(i) put in place appropriate procedures to ensure that the responsibilities for the maintenance of a secure operating environment are properly allocated and discharged;

(ii) ensure that procedures are in place for the physical protection of any equipment to support the services operation. This will, at a minimum, cover intruders, fire, water, environmental (such as storms), and physical damage (accidents as well as deliberate acts);

(iii) implement physical and environmental controls including but not limited to the following:

a. physical entry controls to permit only authorized Bourse Representatives to enter the Bourse's facility and production areas;
b. photo ID swipe cards required for building access;
c. badge controlled entrance/exit devices that physically prevent tail gating;
d. revalidating badge access authorization, at a minimum, every ninety (90) days;
e. processing and printer areas utilized to print confidential/restricted information only accessible by security swipe cards containing photo ID;
f. automatic fire alarm or sprinkler suppression system connected to a central monitoring centre;
g. fire alarm system in place with all the emergency exits armed;
h. visitor logbook for the Bourse's facility and production areas to identify all visitors and the specific Bourse Representative signing in the visitor;
i. logbook for movement of materials in and out of the Bourse's facility and production areas;
j. equipment situated to reduce risks of environmental threats including power failures and damage to cabling; and
k. physical controls to ensure no unauthorized access is gained through non-access points.

(iv) Maintain the following minimum standards:

a. equipment area to be physically secured with controlled access;
b. handheld fire extinguishers easily accessible;
c. automatic fire suppression equipment available and appropriate fire detection equipment installed;
d. water detection equipment as appropriate;
e. appropriate power supply cleanliness and contingency;
f. appropriate environmental controls;
g. appropriate regular cleaning regime;
h. absence of non-utilized equipment;
i. cables properly managed;

j. cables properly labelled;
k. telephone with emergency numbers prominently displayed;
l. contingency plan initiation sequence prominently displayed; and
m. location of backup media prominently displayed close to associated equipment.

4. Operating system security

The Bourse will:

(i) install, configure, maintain and update firewalls, anti-virus and anti-spyware on all devices;
(ii) manage the Bourse's network security infrastructure components used for the connection of the AP and Bourse networks;
(iii) establish procedures for logging, alarming and reporting of network security violations;
(iv) manage and maintain firewalls and gateway devices that connect the Bourse network to the AP network;
(v) employ 24 x 7 network intrusion detection on Bourse network used for LOPR;
(vi) limit access to Bourse-managed software that monitors, manages, manipulates or modifies network configurations and traffic to prevent unauthorized interventions in network operations;
(vii) provide network access control, authentication, authorization and accounting of access to network resources (e.g. routers/firewalls/L3 switches);
(viii) on an ongoing basis, monitor for known vulnerabilities and apply appropriate patches in a timeline that accords with the level of criticality involved and the direction of the relevant third party software provider, and in all cases apply patches in accordance with the software providers' instructions;
(ix) periodically review the Bourse's information risk management requirements for the outsourcing arrangement; and
(x) ensure that all Bourse systems are configured in accordance with industry standards.

5. Access Control

The Bourse will:

(i) at all times operate with strict adherence to secure operational standards, processes and procedures, which will include least privilege for administrator access, and include as a minimum;
    a. clear identification of administration/role types that can be selected with preset rights for each role, such that when an administrator creates a new user, the administrator would assign the user access based on a drop-down menu of roles and not by access function (e.g., read access, uploading files access, etc.)
    b. an audit trail of all administrator actions;
    c. a minimum number of people with privileged access;
    d. maintenance of audit logs;
    e. user control over access to data;
    f. ensuring that Bourse Representatives involved in development of software will not have access to production environment and in all cases separate job functions of Bourse Representatives involved in software development and those Bourse Representatives involved in the deployment, production and support of software; and
(ii) with respect to the Bourse's operating systems, hardware, software tools and network infrastructure systems:
    a. authorize and manage user IDs for Bourse Representatives;
    b. inactive accounts are locked or disabled;
    c. define password rules, including that passwords have a complexity/strength equal to or greater than the standard in the financial services industry and administer

Bourse-owned passwords accordingly, specifically, each user will:

i. use a unique password that may not easily be guessed or obtained by others, that is a password: with a minimum of six characters; without 0, 1, or 3 or more special characters; containing exactly two of the following rules (at least one uppercase letter, one lower case letter; one number; and one non-alphabetic, non-numeric character); and free of consecutive identical characters, letters or numbers (i.e., not be similar to aaa, ababab, 111, 121212, etc.);

ii. be prompted to reset their own password no less frequently than every 60 days; and

iii. advise if they suspect or know that the password has been compromised in any way and change it immediately;

d. control and manage privileged user authorization for the Bourse;

e. revalidate privileged authorizations quarterly;

f. revalidate Bourse privileged IDs;

g. perform a baseline inventory of user session activity including personal (user) and system IDs, logon date and time, logoff date and time and any changes invoked by privileged users and regularly update and revise the inventory; and

h. ensure systems are protected by password protected screensaver or session timeouts (forced logouts) if unattended for a period of inactivity;

(iii) with respect to connection to the AP network:

a. have controls in place to prevent unauthorized access from connected systems to the AP network;

b. monitor procedures and controls in place to prevent external networks or systems from interfering with the operation of the AP network;

c. restrict access to desktop devices in the facility from where the AP systems are accessed to solely those Bourse Representatives who will perform the services or provide desktop support;

d. establish and maintain a timely, secure process to set up new user access for AP designated personnel, advise APs of user IDs and passwords as required, including required password resets, and remove user access;

e. maintain a log of all AP activity; and

f. ensure the use of encrypted lines and encrypt data at rest; and

(iv) with respect to data storage, use at least 128-bit encryption, increasing the standard as industry encryption standards increase.

6. Information Systems Acquisition, Development and Maintenance

The Bourse will:

(i) evaluate new equipment for known vulnerabilities prior to installation if such new equipment is used directly or indirectly in the performance of LOPR;

(ii) secure the new equipment at installation time by changing default support passwords, disabling or removing any unused services, and applying any applicable security patches; comply with defined security controls, testing and backup required for any Bourse-developed support tools to be run in the AP's environment;

(iii) maintain all code related to support tools developed for the AP only within the AP's environment and only following the industry best practices;

(iv) employ industry best practices for secure code development when developing code on the AP's behalf, which is to include a code review for security vulnerabilities when developing code on the AP's behalf;

(v) successfully test all system changes before implementation, with all software testing provided for use with outsourcing arrangement will be fully tested to an agreed standard;

(vi) manage software tests within a structured testing regime which includes as a minimum:

functional testing, integration testing, security testing, performance testing, acceptance testing, independent testing, and regression testing of system software version compatibility;

(vii) maintain procedures to ensure the proper certification and acceptance of products after testing and such software certification will include as a minimum: customer acceptance, design authority acceptance, test certification, and customer handover procedures;

(viii) demonstrate that its testing regime is able to adequately manage test data; and

(ix) not use Confidential Information for testing purposes.

7. Information Security Incident Management

The Bourse will:

(i) employ a process for ensuring that information risk management incidents are properly managed with appropriate escalation processes and documentation requirements;

(ii) respond to requests by the AP for changes to the standards set out herein as external and internal environments change (for example, due to new technologies or regulatory requirements); and

(iii) comply with the AP's requests to establish appropriate actions and timelines to address any security issues.