SECTION 21 CYBERSECURITY AND COMPUTER USAGE POLICY

Altimum Mutuals Inc. recognizes that it is legally required to take steps to protect all devices that contain personal client information so as to protect such information from cyber criminals and cyber incidents.

Altimum has taken steps to ensure that sufficient safeguards are in place to protect the privacy of client information so as to be able to provide its clients with a level of comfort regarding the security of their personal information. Policies regarding cybersecurity and computer usage have been put in place to ensure such protection and to demonstrate that privacy protection is part of the company's business culture. We want to avoid inappropriate or illegal internet use that creates risks for our company and its reputation. Any use of the company's computers must follow corporate policy to ensure that we maintain client confidentiality and protect client data.

The following steps have been taken to accomplish these objectives.

1. Leadership

   Altimum's Chief Executive Officer together with the firm's computer technician/security consultant attended the Fundserv Cybersecurity Seminar.

2. Assessment

   To determine each Approved Person's level of familiarity with the concepts and to identify issues, Altimum had each Approved Person complete a Supplementary Security Assessment Re: Data Breach Prevention and Anti-Money Laundering and Anti-Terrorist Financing Compliance as part of their 2018 rep audit.

3. Training

   Altimum has made its Approved Persons aware of the new data privacy and security regulations effective in Canada as of November 1, 2018 and the firm's obligation to report data breaches. Altimum requires that each Approved Person take a comprehensive Cybersecurity course approved by Altimum which focuses on many cybersecurity and identity theft issues including training regarding phishing attempts to steal data through attachments to bogus, fake emails. All representatives have taken the course as of January 2019.

4. Air-Gapped Computer for Corporate financial record and bookkeeping.

   The company's financial records are maintained and recorded on a computer that has internet access disabled.

5. Redundant Data Backup

   Altimum procured a secondary Canadian data backup centre through On-Deck Hosting. A complete data backup set of all records on the Viefund system is created weekly and stored in a secure facility off-site.

6. Policy regarding disposition of paper records

   Altimum requires that representatives use a cross-cut shredder to adequately dispose of all personal client information.

7. Specific requirements as to Computer Operating System

   Altimum has purchased a computer using the Chromebooks operating system for each Approved Person to use exclusively when accessing client information on the internet. Approved persons are responsible for this company equipment as it remains the property of Altimum Mutuals Inc. Approved Persons are not to attempt to deactivate or configure settings and firewalls on these computers.

   The advantages of Chromebooks are:

   a) Altimum does not need to monitor whether representatives are using the latest updates of the computer operating system because Chromebooks update their OS silently, automatically, and in the background. Therefor malicious attacks that rely upon individuals not keeping their computer systems updated with the latest patches are thwarted and are not a concern.
   b) Altimum does not need to monitor whether the Approved Person is using Anti-Virus software, and whether such software is approved by Altimum, is compatible with the system, is out of date, or whether the subscription to such software has been renewed by the Approved Person because the Chrome OS has built-in virus and malware protection that is always updated to the latest version every time the computer is turned on.
   c) Altimum does not need to monitor use of client data for mortgage business, income tax return preparation, financial planning, life insurance or any other outside activity as the Chromebooks operating system is generally incapable of running Microsoft programs such as Excel and Word, or programs issued by insurance or mortgage companies, that would be utilized in these businesses. But as Viefund is web-based, there is no such issue with that software and it can be run without difficulty on a Chromebook (because in reality it isn't being run on a Chromebook at all.)

8. Encrypted, Password Protected Email

   Altimum has set up a web-based encrypted email account for each representative and Head Office using the technology of Microsoft Outlook through servers located within Canada (Quebec). Our company has the right to monitor all emails. Approved Persons are to tick the Private Computer box when signing in, which is selected by default. By the act of signing into the Outlook website, the Approved Person is confirming the statement in red print on the sign-in page, which reads, "Warning: By selecting this option, you confirm that this computer complies with your organization's security policy." Only the Chromebooks issued by Altimum conform to Altimum's security policy so they are the only computers to be used to access the secure, encrypted email site. All emails are to be password-protected to protect client confidentiality should they be accidentally sent to or recovered by someone other than the intended recipient.

9. Use of Email

Altimum advises our Approved Persons to be careful when downloading and opening or executing files and software. If they are unsure whether a file is safe, they are to ask the Compliance Department for direction before opening it. Approved Persons are not to register to illegal, unsafe, disreputable or suspect websites and services and are not to send obscene, offensive or discriminatory messages and content. They are not to send unauthorized advertisements or solicitation emails. They are not to send confidential client information to unauthorized recipients. They can, however, use the encrypted, password protected email service provided by Altimum to send client statements, etc., or to send orders, KYC information, address updates, etc. to Head Office. The party receiving it is required to use a password to open the email.

10. Elevated Security Settings

Altimum implemented Quad 9 DNS on each Chromebook. As well, Telnet, SSH, UpuP, SnMP, SSDp and SWMP were disabled.

11. Two Factor Identification

Altimum has set up each Chromebook to use two-factor identification and deployed Yubico security keys to be used by each Approved Person when accessing their own Chromebook. Alternatively, their mobile telephone can receive a confirming identifier to be used instead.

12. Passwords

Passwords are to be kept secret at all times and should be unique to the Approved Person's use of Altimum's computer equipment. Passwords are not to be shared with support staff or outside suppliers without express permission from the Compliance Officer.

13. Limited Password Resets

Altimum does not require passwords to be changed regularly, because it has been found that frequent password changes actually reduce security as individuals often use passwords which are easier to remember and which change with the months or the seasons, thereby making them easier to crack. A good solid password which is kept secure is generally safer than a password that undergoes frequent revision.

14. Specific Requirements as to Routers

Altimum purchased new routers to be used by the Approved Persons when using the Chromebooks.

15. Disabled Router Resets

Routers can be set up to be secure, but the reset button can restore original factory settings which can be used to thwart such security measures. The routers provided to the Approved Persons have had the Reset button disabled. Approved Persons are not to attempt to deactivate or reconfigure settings on routers. Approved Persons are responsible for the company's routers used in the course of conducting Altimum business.

16. Specific Requirements as to Printers

Altimum has purchased a dedicated HP printer to be used by each Approved Person but only in combination with the Chromebook provided to the Approved Person. Approved Persons are responsible for the company's printers used in the course of conducting Altimum business, including keeping a supply of ink on hand for the printer at the Approved Person's own expense.

17. Computer and Internet Usage Policy

Altimum has the right to monitor websites visited by our Approved Persons and Employees and the Chromebooks have the ability to do so. Approved Persons are not to download or upload obscene, offensive or illegal material. They are not to visit potentially dangerous websites that can compromise the safety of the computer. They are not to use the company's computer to perform unauthorized or illegal actions such as hacking, fraud, or buying or selling illegal goods. They are not to download or upload music, newspaper or magazine articles, videos, movies, television programs or other copyrighted material and software. They are not to visit Facebook, Instagram, Youtube, Linkedin or other social media sites using the Chromebook. They are not to invade another person's privacy or access sensitive information that is not required to perform their duties.

18. Websites

All websites must be approved and monitored by the Compliance Department. See policy regarding advertising for more information regarding advertising on the internet.

19. Limitation of Liability

If the Approved Person's own personal data is infected with malicious software or is compromised as a result of inappropriate use by its Approved Person, Altimum Mutuals Inc. will not be responsible if a computer other than the approved Chromebook computer was used.

20. Compliance

It is the responsibility of the individual Approved Person to ensure that he or she is in compliance with Altimum's Computer and Internet Usage policy. If for any reason the Approved Person finds difficulty with the software or the hardware such that it is difficult to remain in compliance with the policy, they are to contact the Compliance Department for assistance. Approved Persons who do not conform to this policy will face disciplinary action. Serious violations will be cause for termination of employment or legal action where appropriate.

Altimum Mutuals Inc.

Supplementary Security Assessment Re: Data Breach Prevention

Part I: *QUESTIONNAIRE*

1. Do you use a separate dedicated computer for your Altimum business? (eg. no insurance client files, no mortgage client files, no income tax client files, no youtube, no games, no Netflix, no personal records, no electronic banking, no other email service, no Google searches, etc.)
2. Do you keep electronic copies of client files on your computer?
3. Do you have and regularly use a cross-cut paper shredder?
4. Is your computer secured by a password at startup?
5. Do you shut down your computer each night or when not in use?
6. Do you have a notebook computer?
7. Do you back up data saved on your computer relating to Altimum business?
8. How often do you back up your data?
9. What media do you use to back it up to?
10. Where is your copy of the data backup stored?
11. Is the data backup under lock and key?
12. Do you subscribe to a data backup service?
13. Do you use your computer for internet banking?
14. Do you change your password on Viefund regularly, eg. monthly?
15. What antivirus program do you use? eg. Bitdefender, Kaspersky?
16. Is your antivirus program also installed on your notebook computer?
17. Is your computer connection to the internet by cable or WIFI?
18. Do you use a secure WPA2 WIFI connection secured by a password?
19. Do you ever log into an unsecured network, eg. client's home, Tim Horton's, neighbour's network, family's network while visiting them away from home?
20. Do you use a VPN? (Virtual Private Network)?
21. Do you use Gmail or Outlook or encrypted e-mail? eg. Proton Visionary.
22. Does Altimum's compliance personnel have access to all business email?
23. Do you use external computer support, eg. Geeksquad from Bestbuy?
24. Do you send clients statements or other confidential information by email?
25. Do you use Dropbox or do you use faxing, or Sync.com Business Pro?
26. Have you taken a course on computer and internet security?
27. Is your cell phone secured by a password or fingerprint security?
28. Do you access Viefund from your cellphone?
29. Do you have an antivirus program on your cell phone?

30. Have you given Viefund access to anyone else working with your accounts?
31. Have you used the client/advisor contact system Notification in Viefund?
32. Do you choose client passwords for their accounts? eg. does more than one client have the same password? Do you store their password information?

Note : In cases where data security is at risk, representatives' passwords may be changed by the Compliance Department, effectively locking the representative out of the back office system until appropriate measures are taken to prevent a breach of client data. Client information will continue to be available to the representative by other than electronic means.

Altimum Mutuals Inc.

Supplementary Security Assessment

Re: Data Breach Prevention

Part II: ***ACTION PLAN***

Enter Question Number and Anticipated completion date below.
Where multiple problems exist, set priorities and mark them as *.

Rep Name_____ Rep Signature _____ Date_____

Acknowledgement by Approved Person of Section 21 of the Compliance Manual,

Cybersecurity and Computer Usage Policy

I have read, understood and accepted Altimum's policies and procedures regarding Computer and Internet Usage and have agreed to abide by them.

Representative Name _____

Representative Signature_____

Date _____

Compliance Department Acknowledgement _____

Date received by Compliance Department _____