BRIDGEWATER ASSOCIATES, INC.

TECHNOLOGY USE POLICY

Revised: 10/31/07

TECHNOLOGY USE POLICY

This policy sets forth a basic set of standards for use and protection of Bridgewater's computer and information assets. This policy relates, but is not limited to, computer workstations, servers, laptop computers, electronic mail, databases, networks and connection(s) to the intranet, internet and any other information technology services available both now and in the future.

Information and Information Technology Systems, including the computers, networks, applications (both third party and proprietary), technology facilities and the data housed therein, permit individuals, including all officers and directors, full-time, part-time and temporary employees, interns, consultants, independent contractors and other non-Bridgewater personnel (collectively, "Users") to perform their duties at Bridgewater. Users are not allowed to remove any "Confidential Information" as described in the Code of Ethics from Bridgewater networks or property by any means (including, but not limited to, internet, email, CD/DVD, disk, printed page), without the approval of their department manager (or in the case of non-Bridgewater employees the manager of the Bridgewater department for which they are performing services).

Bridgewater's Information and Information Technology Systems are intended solely for Bridgewater business purposes. Incidental personal use is permissible if the use: (i) does not involve a significant amount of resources that could otherwise be used for business purposes; (ii) does not interfere with a User's productivity; (iii) does not preempt any business activity; (iv) is not contrary to any other Bridgewater policy; (v) does not intentionally make Bridgewater susceptible to excessive spam or unsolicited requests; and (vi) does not disparage or diminish the reputation of Bridgewater or its employees, officers, directors, shareholders and clients. It is the responsibility of each User to ensure that Bridgewater Information and Information Technology Systems are used properly.

Users should not expect electronic communications made or received using Bridgewater's Information Technology Systems to be private. Bridgewater expressly reserves the right to without notice access and examine Bridgewater computer systems and networks and all information stored or transmitted through these systems and networks including, but not limited to, all electronic mail. As such, Users should have no expectation of privacy in the use of Bridgewater's Information Technology Systems. Bridgewater may monitor *all* activity on Bridgewater technology systems, including but not limited to personal uses such as online banking, online health information, shopping, or personal email through the email kiosk. This monitoring may include keystroke logging, screen captures, and Internet activity monitoring, which may reveal personal information such as bank account information, passwords, medical information, or other personal information. Any information obtained by Bridgewater during such monitoring may be used for any appropriate purpose as determined by Bridgewater in its sole and exclusive discretion.

All electronic communications (e.g., email, IM, etc.) made using Bridgewater's networks, computers, systems or other property will be deemed the exclusive property of Bridgewater. All electronic communications are to be written in English. If there is a legitimate business need to send a non-English email or communication, a translation must be provided to Compliance at the time the email is sent. The Corporate Counsel & Compliance Department conducts regular reviews of email and instant message communications. The purpose of these reviews is to ensure that Bridgewater is complying with its regulatory obligations as well as its own internal policies, including the requirement that all electronic communications be consistent with the professional environment that we strive to maintain. All Users are reminded that such reviews will take place and to carefully consider the appropriateness of any statements made by them in any email communication. Users are further reminded that any personal emails sent via Bridgewater's electronic communication facilities will be retained and are subject to review by Bridgewater compliance personnel as well as our regulators.

The use of Bridgewater internal instant messaging for each User must be approved by Department Managers.

The use of web-based email sites (e.g., Gmail, Hotmail, university email, etc.), file upload sites such as Yahoo! Briefcase or Xdrive, personal/home websites, and other web-based publishing sites including blogs is prohibited except via the Email Kiosk Server accessible through Vader. Users should never use or divulge their Bridgewater e-mail address on any public site unless it is being used for business purposes. Notwithstanding the above, all electronic business communications must go through the Bridgewater email servers, with the exception of Bloomberg instant messages. In the event of a Bridgewater declared emergency, the use of personal, web-based email sites (e.g., Gmail, Hotmail, etc.) may be used, however, in all cases Compliance@bwater.com must be carbon copied on every email.

All client-related email should be saved in Outlook under "Public Folders, Client Info" under the name of the relevant client. It is the responsibility of each User to transfer all client-related emails to the appropriate client folder.

All information received, stored or transmitted on behalf of Bridgewater is to be treated as Confidential Information. As such, no internal email may be forwarded outside of Bridgewater unless: (i) there is a specific business reason to do so; or (ii) the forwarded email is about specific Bridgewater benefits or events made available only to your family (or similar close relationship), e.g., emails regarding flu shots or Bridgewater's holiday party.

All electronic communications form a part of Bridgewater's company records. As such, electronic communications may be subject to disclosure to law enforcement or government officials or to other third parties through subpoena or otherwise. Users must ensure that business information contained in electronic communications is accurate, appropriate and lawful.

Moreover, the Investment Advisers Act of 1940 (the "Act") requires that Bridgewater maintain the originals of all written communications (including email) received and copies of all written communications sent to any party, including persons that are not clients of Bridgewater, relating to the business of providing investment services. It is our policy to retain all internal and external email and internal instant messages, as well as all Bloomberg messages. With the exception of internal instant messages using Microsoft Office Communicator 2005, as upgraded, and Bloomberg instant messaging, no other instant messaging is permissible.

Users must conduct themselves in a courteous and professional manner when using Bridgewater's Information Technology Systems, including when using all email and other electronic communications. Users should write all email and other electronic communications with the same degree of responsibility that they would employ when writing letters or internal memoranda on Bridgewater's letterhead.

GENERAL RULES

The following are some basic rules governing the use of Information and Information Technology Systems at Bridgewater:

A. HARDWARE AND SOFTWARE

Bridgewater provides each User with job appropriate hardware and software. The hardware and software are owned and maintained by Bridgewater, which has the right at any time, without notice, to examine and/or confiscate any hardware, software or data maintained on such hardware and/or Bridgewater's Information Technology Systems. If there is a technology device that has not been provided to you that you believe will help you to be more productive in performing your duties, please request it through your department manager.

No unapproved information technology devices should be used in conjunction with Bridgewater's Information Technology Systems. This includes, but is not limited to, other computers, laptops, ZIP drives, Thumb drives, USB drives, memory sticks, CDR/CDRW drives or any other mass storage devices. Exceptions will only be granted on a case-by-case basis, in writing, by a department head and the designated security officer.

Any software installed or data files stored on a Bridgewater computer must be approved in advance by the department's Technology Manager or his or her designee. This includes software and data files downloaded from the internet. Use, downloading, installation and/or storage of illegal or pirated software or files are not permitted in any form. In general, software will be approved if it is properly licensed, intended for a legitimate business purpose, and does not expose Bridgewater to security risks. Non-business related software should not be installed on Bridgewater computers. If you are unsure of what is considered prohibited, please contact the designated security officer.

Department managers may implement additional security measures in high-sensitivity areas such as Research.

B. USER ID AND PASSWORD

Each User must have a User-ID and password prior to being able to use any Bridgewater computer or Information Technology System. A User-ID and a password, both of which are unique to an individual, will be supplied to each User by the Information Technology Department.

Each User is responsible for all activity that occurs on his or her User-ID unless such ID is stolen and it is demonstrated that the User was not negligent in having allowed such theft to occur. User- ID's are revoked when a User is no longer authorized to access Bridgewater's Information Technology Systems. User-ID's are also subject to suspension if not used regularly or if an incorrect password is entered repeatedly.

It is the responsibility of each User to protect the confidentiality of his or her password. Passwords must not be shared with others or recorded in any places where they might be found. The Help Desk must be informed of any actual or suspected password disclosures and will reset the password accordingly. Users are responsible for changing their passwords when prompted by the system.

Users who are provided with other authentication hardware such as a SecurID token or smartcard must take care to protect it and report promptly if it is lost or stolen.

Users must not allow others to use their access without supervision.

C. REMOTE DIAL UP AND VPN ACCESS

Bridgewater provides VPN access to the Information Technology Systems to facilitate work while away from the Bridgewater premises. Access and assigned equipment are provided only by the Information Technology Department upon request of department managers and are intended for Bridgewater business purposes only. Use of remote access is subject to this policy. Users must not share their remote access or allow others to use it either directly or indirectly.

D. DAILY BACKUPS

The Information Technology Department conducts periodic backups of all information that resides on its central computer systems, servers and networks in order to protect Bridgewater's information resources from loss or damage. Maintenance of information stored on a User's personal computer or laptop hard drive (e.g., C: drive) is the responsibility of the User and is not

included in normal backup procedures and recovery capabilities. In case of equipment failure or upgrade, any information on a local system may be lost.

E. VIRUS-SCREENING SOFTWARE

Virus-screening software has been and will continue to be installed on Bridgewater desktop and laptop computers and must not be disabled for any reason. No User may take any steps to disable any firewalls, filters or similar protections which have been installed by Bridgewater. Users may not load onto the Information Technology Systems or transmit any disabling software, such as Trojan horses, viruses, worms, time bombs or any other form of disabling code.

F. LOCK COMPUTER

Bridgewater computers must utilize a screen-saver with password protection, configured to activate after no more than 5 minutes of inactivity, unless an exception is approved by the Security Officer.

Each User must lock his or her computer before leaving at the end of the workday. Users should never leave their computers logged in and unattended.

Users entrusted with Bridgewater computer assets, including desktops, laptops, Blackberries, and software, must exercise due diligence at all times to prevent theft, destruction or other misuse of the assets. Portable laptops, notebooks, palmtops and other transportable computers containing sensitive Bridgewater information must be treated with the same care provided to Bridgewater documents. If a Bridgewater computer or Information Technology device is lost or stolen, the Help Desk must be notified immediately.

G. THIRD PARTY SOFTWARE

No User should include any code that is subject to any open source license in a Bridgewater program, application or file without the prior authorization and approval of Bridgewater's legal counsel. Use of stand-alone open source tools is permitted (if approved per section A) as long as the license is adhered to.

Unauthorized duplication of copyrighted computer software violates the law and is contrary to Bridgewater's standards of conduct. Bridgewater prohibits such copying and recognizes the following principles as a basis for preventing such occurrences:

- Bridgewater will neither engage in nor tolerate the making or using of unauthorized software copies under any circumstances;
- Bridgewater will provide legally acquired software to meet its legitimate software needs in a timely fashion and in sufficient quantities for all Bridgewater computers;
- Bridgewater will comply with all license or purchase terms regulating the use of any software that Bridgewater acquires or uses; and
- Bridgewater will enforce internal controls to prevent the making or using of unauthorized software copies, including effective measures to verify compliance with these standards.

H. TRADING AND OPERATIONS DEPARTMENT SECURITY

Users may not use personal cell phones or business cell phones (including Blackberries) to make or receive phone calls at any time while in the Trading or Operations Department areas (except in emergency situations that do not involve business communications). In the event of a Bridgewater declared emergency, Users in the Trading and Operations Departments must receive authorization from the Management Committee before conducting business on cell

phones. Furthermore, no computers in the Trading or Operations department areas may be connected to external networks such as the public wireless network or carrier broadband networks (such as Verizon Broadband access, or Sprint Mobile Broadband).

I. CONSULTANTS

Nothing contained herein shall be deemed to establish or create an employer-employee relationship between Bridgewater and any consultants, independent contractors or other non-Bridgewater personnel (collectively "Consultants").

- Consultants are not to use personal or other non-Bridgewater owned laptops or computers at any time for the purpose of doing Bridgewater work unless explicitly authorized to use the VPN Sandbox and all work must be completed within VPN rather than completed locally and sent to Bridgewater. Consultants may not use instant messaging software (other than internal Bridgewater Microsoft Office Communicator, if provided) while on-site at Bridgewater facilities.

- Consultants must make any technology device brought into a Bridgewater facility or used for Bridgewater business available for inspection to Bridgewater security personnel if requested due to a suspected security incident or random audit.

J. POLICY COMPLIANCE AND REPORTING

All Users are responsible for complying with this Policy and for immediately reporting any known or suspected violations to their immediate supervisor or to the Chief Compliance Officer. Users must not circumvent or attempt to circumvent Bridgewater security controls or disable security software installed on Bridgewater systems.

Exceptions to this policy must be approved, in writing, by the Chief Technology Officer or Information Security Officer.