ADVISER

IT Policy v1.3

Information Technology Department

PIAS

PROFESSIONAL INVESTMENT ADVISORY SERVICES

1. REVISION REGISTER

Revision Number	Date of Update	Reason for Revision	Reviewed / Approved by	Actioned by
0.1	Sept 2018	Creation of Adviser Handbook	Lindy Tan	Roy Tan
0.2	Oct 2018	Revise phasing of IT policies	Lindy Tan	Roy Tan
1.0	Aug 2019	Updated IT policies	Lindy Tan	Roy Tan
1.1	Feb 2021	Updated IT policies	Roy Tan	Weimeng CAI
1.2	July 2021	Updated e-mail encryption	Roy Tan	Weimeng CAI
1.3	Dec 2022	Updated IT policies	Roy Tan	Weimeng CAI

2. INTRODUCTION

The Information Technology (IT) Policy applies to all advisors within Professional Investment Advisory Services Pte Ltd (PIAS), and other company that may come under the management oversight of PIAS presently and/or in the future, including all their subsidiaries, affiliates and external offices.

This handbook is also intended as a general reference tool for advisors. It contains only general information and guidelines. It is not intended to be comprehensive or to address all the possible applications of, or exceptions to, the general policies and procedures described. For that reason, if you have any questions concerning on the applicability of a policy or practice to you, you should address your specific questions to the Information Technology department.

The Company reserves the right to review and modify the policies, rules and regulations from time to time as appropriate.

2.1. Objective

This policy sets the terms to govern the proper usage of PIAS's Information Technology Systems.

2.2. Scope

This policy applies to all Advisors including all Personal Assistant and Administrative Staffs of the PIAS.

3. POLICY

3.1. Acceptable Use

This is to outline the acceptable use of IT equipment at PIAS. These guidelines are in place to protect the advisors and PIAS. Inappropriate use exposes PIAS and advisors to risks including virus attacks, compromise of network systems and services, and legal issues.

- Advisors shall use PIAS's IT systems for business purposes only.
- Advisors shall be mindful not to disclose any sensitive or confidential information.
- Advisors shall not access data or applications that he/she is not authorised to access.
- Advisors shall not attempt to exploit or probe for security loopholes on PIAS's IT systems or other organisations' network.
- Advisors shall not attempt to circumvent data protection schemes and shall report any security loopholes to IT department.
- Advisors shall not attempt to launch denial of service attacks or perform any activity that would degrade the performance of PIAS's IT systems.
- Advisors shall not attempt to introduce any malware (e.g. computer viruses, worms and Trojan horses) to PIAS's IT network.
- Advisors shall not assist anyone to cause damage to PIAS's IT systems.

Advisors shall not use PIAS's IT systems to carry out any unlawful or illegal activities (e.g. unauthorised access to computer systems or network accounts and acts of sexual harassment) and their actions are subject to the relevant legislation such as the Singapore Computer Misuse Act, Evidence Act, Electronic Transaction Act, Copyright Act and Spam Control Act.

3.2. Account and Password Management

These guidelines are to educate advisors on the characteristics of a strong account password as well as to provide recommendations on how to securely maintain and manage account passwords.

- Account sharing is strictly prohibited.
- Every user is assigned a unique user id and he/she is accountable for his/her account.
- Password shall meet the following complexity requirements:
- At least 8 characters
- Contain characters from three of the following four categories
    - Upper case characters (A-Z)
    - Lower case characters (a-z)
    - Numeric characters (0-9)
    - Symbols (e.g. #, %, &, @)
- Password shall be changed at least once every 90 days. It shall be different from the previous 5 passwords and existing password.
- Advisors shall take precautionary measures to safeguard his/her password and it shall not be disclosed to any other person.

3.3. Software/Hardware

These guidelines are to educate advisors on the need to protect sensitive information and prevent its inadvertent disclosure. Data breaches can lead to significant financial losses and reputational damage.

- Advisors shall not use unauthorised or unlicensed software.
- Advisors shall ensure all software is updated with the latest security patch.
- Advisors shall ensure that the virus scans in their IT systems are enabled and the virus signature files are updated regularly.
- Advisors shall disconnect their IT systems from the PIAS network if they suspect there is a computer virus infection.
- Advisors shall not connect any unauthorized network devices (e.g. switch, router, access point) into PIAS network.
- Advisors shall use the Windows Lock to lock their PCs/Notebooks before leaving their desks *[by pressing the "Windows Logo" key + "L" key concurrently].*
- Advisors shall ensure that confidential information is minimally password protected and the password is transmitted separately from the protected file.
- Advisors shall physically secure their notebooks with the cable lock when the notebooks are left unattended during work hours and store their notebooks in locked storage before leaving office at the end of the day.
- Advisors shall not leave any sensitive or confidential information unattended on printer, copier and fax machine.
- Advisors shall destroy any paper waste, which may contain sensitive or confidential information, using the documents shredder.
- Advisors shall treat mass storage devices such as CDROM, DVD or USB drives as sensitive materials and secure them in a locked location.

3.4. E-mail System

This is to covers appropriate use of any email sent from a PIAS email address. These guidelines are in place to protect the public image of PIAS reputation.

- Each advisor shall respect the intended official usage of the PIAS's email system.
- Advisors shall not send forged e-mail that will intimidate or harass other Advisors, chain messages that can interfere with the efficiency of the system, or promotional mails for profit-making purposes.
- Advisors shall not send unsolicited e-mails using the PIAS-assigned e-mail address. Sending large volumes of unsolicited e-mail to overload and attempt to disrupt the e-mail system is prohibited.
- Advisors shall not send messages that contain obscene, offensive or slanderous material.
- Advisors shall not break into another user's electronic mailbox or read someone else's e-mail without their permission.
- Advisors shall ensure e-mail attachments and files downloaded from the Internet are scanned for viruses before execution.
- Advisors shall not open e-mail attachments from unknown or untrusted sources.
- Advisors shall not enable any 'auto-forwarding' rules to send official e-mail to any e-mail addresses outside of PIAS.
- Advisors shall not use personal e-mail system (e.g. Hotmail, Yahoo, or Gmail) for sending official e-mails.
- Advisors shall not use e-mail to register for non-work related application.
- Advisors shall ensure that e-mails that contains confidential attachment should be encrypted with password.
- Advisors shall ensure that password to encrypted e-mails should be shared using a different e-mail or other medium like SMS. Password should not be included together with the encrypted attachment.

3.5. Internet Access

This define standards for Internet access from any host within PIAS's network. These guidelines are designed to ensure advisors use the Internet in a safe and responsible manner, and ensure that advisors internet usage can be monitored or researched during an incident.

- Internet access shall not be used for personal or private gain.
- Advisors shall not access any web sites containing objectionable content. In addition, objectionable information, messages or posting as defined by the Singapore Laws shall not be uploaded to / downloaded from, sent or posted on the Internet respectively.
- Advisors shall not copy programs or data protected by copyrights or by special license and any downloaded files shall be screened and verified by virus detection software before activation.
- Advisors shall not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property rights, including the installation, distribution or used of any software that is not appropriately licensed for use by the user.
- Advisors shall not transmit any offensive materials including but not limited to defamatory comments, personal insults, obscenity over the internet.
- Advisors shall not transmit the PIAS information to web-based file sharing platform.
- PIAS reserves the right to allow authorised staff/vendor to monitor Internet access, use of PIAS's electronic mail systems, and examine the information stored within.
- Should PIAS discover any advisors engaging in prohibited actions resulting in compromise of information security, PIAS reserves the right to temporarily/permanently suspend that user's access and usage of PIAS information resources.

3.6. Third Party and Outsourcing Service Providers (SP)

This ensure the identification and management of IT System implemented third party and outsourcing service providers. Risk associated with the outsourcing IT system should be appropriately identified and where applicable, due process and diligence have been followed and mitigated.

- Advisors shall have a formal contract with SP on the outsourcing services.
- Advisors shall have a separate non-disclosure agreement (NDA) with SP.
- Advisors shall conduct evaluation on SP which will include:
    - SP's business reputation
    - SP's financial standing
    - SP's compliance standards and framework
- Advisors shall update the inventory list of outsource IT systems including the location of where the data are stored and secured.
- Advisors shall ensure business continuity plan is in place with SP.
- Advisors shall ensure data protection plan with SP.
- Advisors shall be responsible for managing the access provided in the SP's system.
- Advisors shall only permit remote access arrangements via secure encrypted networks.
- Third party cloud computing services must have tools in place to monitor and log activity and respond to malicious attack.
- Advisor shall inform PIAS IT on Outsource IT System workflow and process.
- Outsource IT System which deem as MAS Critical System or is Internet facing and hosting customer related information must have multi-factor authentication implemented for login.
- Outsource IT System shall be implemented base on MAS Technology Risk Management guideline.
- Outsource IT System shall be comply with the MAS Cyber Hygiene Notice.