CYBERSECURITY POLICY

The purpose of this policy is to set forth policies and procedures designed to safeguard Optivise Advisory Services (OAS), its advisers, and its client's data and confidential information. This policy applies to all of OAS's IARs, IAR office staff, and employees hereinafter referred to as "Covered Persons."

ELECTRONIC COMMUNICATION

It is the policy of the OAS that all business-related electronic communication sent by a Covered Person is to be sent from an OAS-approved email account. OAS-approved email accounts are defined as any email account set up by OAS for its IARs, its employees or contract consultants, or any other email address that has been approved by OAS's compliance, in writing, to conduct investment advisory business. All email accounts must have the ability to be archived and monitored by an OAS-approved vendor.

Any email account/address that is not an OAS email account and has not been approved by the compliance officer of OAS will be considered to be out of compliance and in violation of this policy for the IAR.

All client/account documents (CAD) that contain account and client information sent by a Covered Person must be sent secure or encrypted. IARs are required to submit all electronic client/account documents to the Home Office of OAS via Elements, the Firm's shared Google Drive, or through a similar encrypted system. Any CAD documents submitted by email will not be accepted or acted on by OAS and will be considered not in good order. Any client loss associated with a not in good order ("NIGO") submission will be the responsibility of the IAR. Violations of this submission policy may result in disciplinary action up to and including termination for cause.

When sending CAD electronically to a client for review and/or signature any file attachments must be encrypted or secure.

ELECTRONIC DEVICES

All IARs of OAS are independent contractors and are allowed a wide amount of latitude in determining which electronic devices are most appropriate and useful for servicing their client's

needs and managing their practice. OAS does require that its IARs maintain the following standards for all electronic devices used for business purposes;

1. All devices used for business purposes must be equipped with antivirus software that is updated and continually running;
2. All operating systems (OS) must be updated to the most current version for that operating system. This is not intended to mandate that an IAR must upgrade from Windows 7 to Windows 10, but that the current version of Windows that you are operating is the most current available version of that product;
3. All browsers: Internet Explorer, Chrome, Safari, Firefox, Onion, etc. must be the most current version of that browser;
4. All devices used for business purposes must have a password or biometric protection feature activated; and
5. If an IAR operates a WiFi network, the network should be password protected.
6. It is recommended that all electronic devices operate through a VPN connection when possible. The Firm currently has an agreement through NordVPN Teams that is available for IARs to use.

PASSWORDS

All passwords for email, CRMs, custodial platforms, aggregation software, etc. (sensitive systems) should have a password that is unique to that system and should not be a simple variation of other passwords used. A strong password should contain both upper and lower-case letters, numbers, and special characters.

All passwords used should be unique to the user, and the OAS expressly prohibits sharing passwords with any other person.

DOCUMENT STORAGE AND RETENTION

All IARs are required to retain all CAD documents on Egnyte, the Firm's shared Google Drive, Omni, or LifeArcPlan. Storage of these documents by other electronic means is not authorized by the OAS. Please note that certain customer relationship management programs (CRM) allow for the storage of documents and client-sensitive information. Before using any CRM to store this information, it must be approved by OAS's compliance officer. All data and information related to any other CRM must be stored on CRM servers and not on the Covered Person's electronic devices. OAS has approved the following CRM systems:

- Redtail
- Omniscient

During the course of business, CAD may temporarily be stored on a portable device, such as a flash drive. This practice is acceptable provided that the information on the portable device is encrypted at a minimum level of 256 bits.

REPORTING

If a Covered Person suspects that a password or an electronic device has been accessed by an unauthorized person, they should immediately change the password(s) compromised and notify OAS's compliance department.

PASSWORD STORAGE

All Covered Persons are prohibited from storing their passwords on an electronic device or in electronic format. This would also include the use of password storing features associated with web browsers and other programs. The use of stand-alone programs such as LastPass is permitted. If a Covered Person wishes to use a password storage program other than LastPass, the program must be reviewed and approved by OAS compliance prior to its use.