SELWOOD
ASSET MANAGEMENT

# DATA SECURITY, RETENTION & CYBERSECURITY PROCEDURE

| POLICY REVIEW LOG | |
|---|---|
| Created | November 2021 |
| Last Update | November 2021, November 2022, November 2023 |
| Review Frequency | Annual |
| Next Review Date | November 2024 |
| Ownership | RCCI |
| Approval | RCCI |
| Policy Location | R:\3. Compliance and Policies\1. Policies\1. Approved Policies |

| | |
|---|---|
| Reference: | EU Delegated Regulation 2017/565 Art 76<br><br>Art L533-10(5) of the Monetary and Financial Code |
| Summary: | Firms are required to store and process personal data in certain way. In addition, firms are required to keep data secure. |

# 1. Data Security

**Mitigating Risk of Financial Crime**

- The Firm holds personal information relating to its staff for HR recording and monitoring purposes.
- The Firm holds customer data relating to its Clients and Investors.
- The Firm does not disclose non-public information about its Client(s) (present or former) to anyone, except as permitted or required by law.
- The Firm has adopted detailed procedures and controls to identify and manage the risk of breaches of information security, of which all Personnel are aware.

**Procedures and Controls**

The following procedures and controls have been adopted and implemented based on the nature of the information gathered, created and maintained by the Firm and the extent of risk to that information, to ensure the integrity, security and confidentiality of such information.

Physical Security

Building maintains restricted access to its premises 24/7/365. All staff will use two different electronic swipe cards to access the building and the office at all times. The firm maintains a clean-desk policy for all staff.

Governance
The firm will notify affected clients promptly after information loss, informing them what information has been lost and how the loss occurred.

Staff Recruitment
The firm vets all new Personnel applying a risk-based approach, taking into account information security and other fraud risk (enhanced vetting criminal records and financial sanctions lists).

Educating Staff

The firm has an ongoing awareness campaign that focuses on the financial crime risks arising from poor information security, as well as the legal and regulatory requirements to protect information.

Passwords
The firm ensures individual user accounts, requiring passwords are in place for all systems and quarterly updated. All staff use password standards at least equivalent to the recommended standard - at present, the recommended standard for passwords is a combination of letters, numbers and keyboard symbols at least seven characters in length and changed regularly.

Taking Information Offsite
The firm prohibits copying of Client information and trading data to portable media unless there is a genuine business reason for it.

Backing Up Data
The firm conducts due diligence on third parties that handle backed-up customer data.

Disposal of Client Data
The firm ensures all paper-based Client data and trading data is disposed of securely by Personnel, using shredders.

Managing Third Party Suppliers
The firm conducts due diligence on all third-party suppliers on their information security standards.

Ongoing Vigilance
These procedures are designed to minimise the Firm's information security, integrity and confidentiality risks, and must be followed by all staff. Where information security, integrity or confidentiality is breached the Firm will take action to remedy the situation and in certain circumstances notify the AMF.

## 2. Data Retention for Compliance

Set out below are the Firm's retention periods for different types of data:

| Type of Data | Reasons for Retention | Retention Period |
|---|---|---|
| Personnel Data | Personnel data is predominantly retained to comply with legal and tax obligations and also for regulatory reasons. | Generally, 7 years. |
| Investor Data | Investor data is predominantly retained to comply with legal and tax and anti-money laundering obligations. | Up to 7 years. |
| E-mails | Emails are archived by Abacus and fed into the SteelEye surveillance. SteelEye has advance indexing and supports searching by specific patterns | All E-Mails are archived for a |

| | | |
|---|---|---|
| | for compliance and allows for policies to be set up. Emails deleted by users are retrievable from the archive. Simple and easy indexing and searching of files | period of 7 years. |
| Call Recordings | All calls are recorded and stored in a format that cannot be alternated. This solution is being provided through Abacus IT by CallCabinet and is also ingested into SteelEye. Simple indexing and searching of files. | All calls are retained for 7 years. |
| MS Teams Recordings / Chats | All Teams chats and calls are recorded and stored in a format that cannot be altered. This solution is being provided by Steeleye. | All calls are retained for 7 years. |
| Bloomberg Messages | Selwood uses SteelEye for Bloomberg surveillance and message archiving. SteelEye stores data in a write-once-read-many (WORM) format in multiple data centers running hot-hot for guaranteed disaster recovery. | All Bloomberg chat and instant messages are archived for a minimum of 7 years. |

The Firm considers the document its retention periods reasonable and consistent with the applicable laws and proportionate in the light of the Firm's size and complexity of operations, the make-up of its clients and counterparties. In order to retain this data securely, the Firm has sought to apply organisational and technical security measures, including computer safeguards and secured files and buildings.

## 3. Cybersecurity Management

Selwood Asset Management (France) SAS elects to follow the Cybersecurity strategy of the Selwood Group ("**Selwood Group**"). Selwood Group is conscious of growing cybersecurity threats globally across industries, including the alternative investment management industry.

Selwood Group regularly reviews its IT framework with Abacus and external consultants for protecting its infrastructure. There were no cybersecurity breaches up to November 2021.

Penetration testing and security audit of the IT infrastructure are conducted every month by an external company. No breaches were reported.

**Prevention**

Selwood has taken a number of steps to prevent and mitigate cybersecurity threats, including:

| | |
|---|---|
| **Education and Training** | ✓ Employee education and training remains one of Selwood's core components in its robust cybersecurity plan<br>✓ Trainings are given to all staff periodically<br>✓ Regular phishing tests are conducted to increase awareness |

| | |
|---|---|
| **Auditing, Monitoring, Detection** | ✓ All network activities are logged including devices connected to the network inbound & outbound traffic<br>✓ Anti-Virus software (SentinelOne) installed on all servers and workstations and monitored by Abacus<br>✓ Network protected by Firewall with built-in Intrusion prevention (IPS), Antivirus and anti-phishing filtering<br>✓ Multi-layer protection on E-mail exchange server |
| **Personnel & Documentation** | ✓ Selwood Group has appointed Patrick Donohoe as the Information Security Officer (ISO) at Group level<br>✓ Fares Bouanika and Guillaume Merle are following IT concerns for Selwood France<br>✓ Business Continuity Plan<br>✓ Written Information Security (WISP), Data Security Breach/Incident Management Policies (for the Group level) are available |
| **Encryption** | ✓ Secure Point to Point connection to the Abacus Private cloud over a Zayo circuit<br>✓ Secondary circuit goes out to the internet via the Abacus cloud so ALL traffic is routed via Abacus multi-layer security<br>✓ Secure access via Citrix XenApp and Citrix Desktop for remote connections and multi factor authentication<br>✓ Secure Sockets Layer encryption for E-mail transmission<br>✓ Secure FTP (SFTP) for sending/receiving trading data |
| **Security, Prevention & Access Control** | ✓ Secure Point to Point connection to the Abacus Private cloud over a Zayo circuit<br>✓ Secondary circuit goes out to the internet via the Abacus cloud so ALL traffic is routed via Abacus multi layer security<br>✓ Secure access via Citrix XenApp and Citrix Desktop for remote connections and multi factor authentication<br>✓ Secure Sockets Layer encryption for E-mail transmission<br>✓ Secure FTP (SFTP) for sending/receiving trading data |
| **Network & Device Management** | ✓ Firewall activated and monitored with alerts<br>✓ All unwanted software are removed from staff workstations<br>✓ All default settings have been changed including router, firewall and access point username/passwords<br>✓ Unwanted automatic software is disabled. All new updates are tested before installed on servers & workstations<br>✓ All removed or unwanted user accounts are deleted from workstations and network accounts<br>✓ Anti-Virus software is monitored by Abacus and regularly updated<br>✓ Encrypted Wi-Fi only available in guest-mode for internet access (separate VLAN) to protect local network<br>✓ Penetrating testing by a third-party (independent of Abacus) is undertaken regularly - > Drawbridge |
| **3rd party / Service provider review** | ✓ All critical service providers are identified, and measures taken, to minimise 'backdoor' cybersecurity threats<br>✓ All risks associated with confidential communication and share of data is assessed with critical service providers |