Information and Data Security Questions and Answers

Advance by Embark is a trading name of Sterling ISA Managers Limited (SIML), a wholly owned subsidiary of Embark Group.

How do you ensure that client data is protected and your systems are secure?

We take our data protection obligations extremely seriously and the security of our customer data is very important to us. We rely on personal data to accurately and effectively assess risk and provide customers with investment opportunities that meet their needs. We are ensuring that our alignment on regulatory interpretation enables continuing delivery of GDPR compliance, specifically taking care of the individual's rights and freedoms, transparency of their data processing and, where applicable, carrying out Privacy Impact Assessments.

All SIML employees receive periodic training with respect to data protection and privacy. Specific training is provided to individuals working in areas that interact with high volumes of personal data (including handling data subject requests) and sensitive personal data. SIML's relevant policies and procedures include authority and access limitations and compliance with data retention requirements.

Fraud prevention is a key activity at SIML, including safeguarding against identity fraud. We have a suite of internal training and support materials that staff absorb on a repeated basis, to mitigate against such fraudulent activity. For security reasons, we do not externally divulge details of infiltration attempts, but promptly act upon any instances to further bolster our controls. Indeed, our framework of controls that ensure we adhere to our regulatory requirements encompass all financial crime, including anti-money laundering, tax evasion, fraud, anti-bribery and corruption. These controls are rigorously tested and monitored regularly to ensure they remain fit for purpose.

For our customers SIML will:

- keep their data safe
- never sell their personal data
- not share their personal data without being transparent about it
- put their data to work so we can better protect them, and so they can get the most out of life.

With regard to the Advance by Embark Platform, this transparency initiative should reassure advisers and their clients that SIML takes its data protection responsibilities seriously and will continuously focus on safeguarding clients' rights in the spirit of relevant legislation and regulation.

How robust is your Information Security Management System?

Embark Group has an information security management system that is approved by the Group Board and operated and managed by a dedicated security manager working alongside our risk and compliance team. Our compliance and assurance standards are measured against our ISMS framework which is aligned to ISO 27001 standards and our internal information security systems are certified to the Cyber Essentials accreditation standard.

Our framework of policies and processes includes data and information security, and the usage of IT equipment and assets. Embark Group Policies include, Information Security, User responsibilities, Remote access, Data protection, and Physical security. Internally, we have mandatory Information Security, and Data protection training for all staff that is repeated annually.

Our security assurance function manages Third-Party suppliers who are contractually bound to provide regular security assurance reporting demonstrating that they adhere to ISO 27001 standards and our externally hosted IT systems are all located in security accredited data centres.

Embark Group also carry out regular assurance testing of our external facing IT systems by utilising an independent, Crest accredited, third party to perform penetration and vulnerability assessments.

What controls and risk assessments do you place on third parties?

Embark Group IT providers comply with our contractual obligations relating to data protection and information security controls. As part of these requirements they provide regular assurance reports against their own ISMS through quarterly reporting and regular audits.

Our business processing partners host all systems in ISO27001 accredited resilient data centres running robust recovery procedures and data backup processes. These strategies alongside our infrastructure technologies including replication and, network redundancy ensure the integrity and availability of our systems platforms at all times. Embark information security monitor our partners' security through regular assurance reporting and management reviews. Our partners are also externally audited as part of their own ISO operational assurance processes and these reports are provided to Embark Group to review.

How are your network and servers protected against external threats and attacks?

Our infrastructure is secured using security defence in-depth principles and a layered approach to IT security. It is regularly tested and assured via external testing through independent third parties. The external network perimeter is protected utilising IDS and IPS technologies and all network traffic for system access is encrypted. In addition, network segregation is employed, and a monitored high availability Cisco firewall solution is in place along with server endpoint protection and hardened Microsoft systems which are updated monthly in line with Microsoft best practice guidelines, system activities are transaction logged. Daily backups are encrypted using 256-bit AES and stored in an offsite secure location.

Business applications are hosted within a Microsoft Azure cloud which conforms to ISO 27001 standards for Cloud Hosting, Business Continuity, and Information Security along with the ISO9001 quality standards.

How do you respond to a cyber security incident?

Embark Group has a formal incident reporting, management and resolution process with a defined set of response levels and escalation paths depending on the severity of the event.

The IT Security Compliance manager would manage and co-ordinate any security events and issues in line with our security Incident policy. Our security function works alongside our IT support function to ensure an effective and immediate response to any threats and incidents resulting from a technology-based threat. Additionally, working alongside our Risk and Compliance team, ensures that a formal escalation governance and a reporting structure is in place for any event that may impact the Confidentiality, Integrity or Availability of our data.

A well-defined Crisis Management Team process is also in place across the group that would be invoked depending upon the impact and risk assessment of any threats or security events.

What data recovery, business continuity and disaster recovery plans do you have?

Data recovery

Our business processing systems are hosted across resilient dual data centres to ensure the integrity and availability of our platforms at all times. These data centres are ISO27001 accredited and perform regular data recovery and failover testing as part of their annual assurance and monthly operational activities.

Our application services are hosted within a Microsoft Azure cloud which conform to ISO 27001 standards for Cloud Hosting, Business Continuity, Information Security along with the ISO9001 Quality standards.

Across our Group Businesses regular Business Continuity reviews are conducted ensuring that processes, plans and communication, both internally and with our Third-party vendors are current and tested.

Business continuity/disaster recovery

Within Embark, the importance of Business Continuity Management (BCM) is recognised and reflected in the Embark Operational Risk Management Policy and the Business Continuity and Disaster Recovery Policy. BCM offers a way to manage some of the operational risks that arise from people, processes, systems and external events. Embark has a robust BCM framework in place. The BCM framework is in line with Group Risk policy.

Embark's business continuity planning incorporates five major business disruption events:

1. Change-oriented scenario causing material disruption
2. People-oriented scenario, where there is a material loss of staff availability
3. Building-oriented scenario, where there is a material loss of premises
4. Infrastructure-oriented scenario, where there is a material impact on technology infrastructure
5. Third Party-oriented scenario, where there is a material impact caused by a Third Party failure

Business continuity (BC) plans are reviewed on an ongoing basis and are tested annually. We maintain a comprehensive set of BC plans covering all critical aspects of our operations – and all aspects of TCF are considered in these plans to specifically ensure Embark delivers fair outcomes, even in the event of a serious incident causing business disruption.

Are staff user privileges and data access rights controlled?

Embark Group manage Identity and Access Management (IAM) on the principle of least privilege access. Application, system and network access is managed centrally via our IT function and all users have unique IDs and passwords.

Well-defined processes for joiners, movers and leavers ensure these processes are maintained and regular audits of user roles and permissions are undertaken as part of operational assurance. Separation and segregation of duties is enforced as part of our access control processes and these are monitored through monthly reviews and management of user entitlements.

What security measures are in place in relation to staff working from home (or remotely) and using removable media?

Remote access is permitted for approved users only and is strictly via corporate SSL VPN, or secure remote desktop connections.

Use of removable media (USB and optical ports/drives, etc.) is disabled by default through corporate policies. Usage of external media is by exception and requires senior management approval and when media devices are approved encryption is enforced.

How do you ensure staff are not a security risk?

All candidates who are issued an employment contract are vetted as part of the pre-employment screening process, in line with legal requirements and regulatory obligations.

Vetting is inclusive of: identity checks, reference checks, criminal record checks, right to work in the UK compliance and credit checks.

Additional vetting/assessment may be required for specific roles or responsibilities.

All staff (permanent, contract and temporary) are required to undertake a suite of mandatory online training (including Data/Information Security, GDPR, Anti-Fraud and Money Laundering, Financial Crime) and associated knowledge confirmation assessment on joining and then annually as a minimum. Further targeted training is provided for specific roles, such as CASS.

All staff are contractually required to comply with policies and standards. Failure to comply with, or breaches of, the relevant IT and security policies would be investigated and may result in disciplinary action – up to and including dismissal.

How do you manage the risks associated with fraudulent email instructions?

Embark Group have anti malware, spam and malicious content technology tools in place to detect and quarantine potential email threats. We also provide training to all staff on how to identify suspicious emails, including fraudulent or phishing emails.

This includes maintaining alertness regarding unusual requests and spotting external attempts to expedite payments apparently sanctioned by senior executives, but which actually originate from criminals.

Employees are expected to forward all suspicious emails to our IT support team on a 'better safe than sorry' basis, and then immediately delete these messages from their inbox. The team will respond with information either confirming the attempted fraud or malicious intent (including malware incursion) or in some instances that the email is in fact legitimate.

Regular monitoring and review of email traffic and any suspect emails reported to our IT service desk is undertaken and where opportunities for improvement or further education are identified these will be addressed appropriately.

How do you ensure a payment instruction is genuine?

We have a robust anti-fraud control environment. Many of our BAU controls are in reality good anti-fraud controls too.

There are a number of controls around payments out, as our primary aim is to ensure our customers' assets remain safe and end up with our customer and not the fraudster, so the priority action is to verify payment requests.

Examples of controls in place:

- Risk Based Modelling (RBM) – identification of factors that influence payment out checks, e.g. level of claim, length of claim, value of claim, type of product; there is a payment out authorisation checklist in use.
- The RBM restricts third-party payees to those who can be easily verified; payee must be one of the following: 1. A Solicitor (whose name, address and client asset/money account set-up has been verified on The Law Society website and payment is made to the Solicitor's client account. 2. Other insurers as applicable, whose name and address has been verified on the FCA website and the payee includes the full name of the insurer together with the customer name/account number. 3. The IFA, whose name, address and client account set-up has been verified on the FCA website and payment is made to the IFA's client asset/money account. In addition, where a written request from the account/policyholder is received and third-party ID checks have been performed, payments can be made by cheque to a nursing home or school.
- Identification and Verification process.
- Checking customer signatures is a key anti-fraud control in certain scenarios.
- The party involved is contacted by a means other than email to confirm details.
- Where a change of bank account details is requested, contact is made by phone or letter to confirm if they have asked for this change. We do not use the contact details provided in the letter or email requesting the change unless these have been verified as correct.
- Where bank details are received via email, we ensure that this emanates from the legitimate email address of the party involved.
- Anti-Fraud letters – e.g. letters sent to the old and new address advising when the address was changed or double checking with the servicing agent on our Advance by Embark Platform.
- Call handler scripts.
- Proof of existence letter.
- Payment thresholds.
- Reconciliations.
- Our staff minimising their work references on social media (e.g. omit role); fraudsters are known to perform online research of organisations, their CEOs and the employees in Finance departments.

Additionally, our internal training, education and awareness campaigns encourage suspicions to be reported if any of these fraud indicators are flagged:

- Overseas death and/or payment to new or foreign bank account.
- Inconsistent factors – e.g. cause of death inconsistent with lifestyle.
- Change of address and/or bank details shortly before surrender request.
- Different addresses on joint-life plans.
- Divorce/separation on joint plans followed by surrender.
- Signature forgeries.

- Numerous phone calls for information prior to surrender.
- Request to pay one party only on joint life policy.
- Customer resident in high risk country – e.g. South Africa has a known issue with postal interception, which can lead to Life Surrender Fraud.
- Customer receiving annuity at unusually old age (e.g. late 90s/early 100s).
- Language, spelling, style – is it consistent with what we would expect.
- Recipient of funds is not contactable – apparently ill, working abroad, or on holiday.

As indicated previously, on the Advance by Embark Platform it is the advisers who are responsible for ensuring that they are dealing with their genuine clients, and acting on valid instructions from those clients. The advisers also determine the communication and view preferences for their clients. The Platform Terms of Business expressly informs advisers that we are not obliged to check any information they input on the Platform (and this will include changes to their client's personal details), and also that the adviser is liable for any losses caused if they provide us with inaccurate information. We prompt advisers to check payment out requests.