|  |  |
| --- | --- |
| **Policy Title** | **Information & Cyber Security Policy** |
| **Owner** |  |
| **Version Number** |  |
| **Primary Audience** |  |
| **Document Location** |  |
| Objective | |
| This policy sets out the minimum standards to be followed to protect the information we hold from unauthorised access and/or change, including as a result of cyber threats. | |

|  |
| --- |
| CONTEXT |
| Business Context |

[company] is committed to achieving our strategic objectives through a commitment to our Purpose, Vision and Values, all of which have been carefully considered and crafted to put the client at the heart of our business. To achieve our business objectives, [company] holds a considerable volume of business specific and client information, some of which is sensitive in nature. [company] is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

Given the internal and external threats that all firms face, the information we hold is at risk of being stolen, copied, lost or otherwise compromised resulting in client detriment, and adverse legal, regulatory, financial, reputational and/or other consequences for the business. This may be caused internally or externally, deliberately or accidentally, and it may relate to information held or transmitted on any media, including that held or processed on IT systems or devices, on paper or other 'hard' format.

Therefore, it is essential that we have a strong framework of controls in place to ensure that this information is professionally managed and protected.

This policy sets out our minimum requirements that must be followed to ensure we protect our data from unauthorised access and cyber threats.

|  |
| --- |
| Regulatory Context |

[company]’s requirements for meeting its obligations under the UK General Data Protection Regulation as well as the FCA’s expectations regarding how it collects, manages and secures client data are set out in the Data Protection and Privacy Policy.

In relation to information and cyber security, under Retained Regulation (EU) 2016/679, UK General Data Protection Regulation (UK GDPR), [company] must:

* use technical or organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;
* implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into [company]’s data processing activities; and
* be able to demonstrate that it has used or implemented such measures.

[company] must also meet the Operational Resilience requirements as outlined in FCA SYSC 15A.2 relating to the effects of plausible disruptions to its business services, considerations should be given to the following factors including but not limited to:

* The nature and size of the client base
* The sensitivity of data held.
* Impact on the financial position and or reputation of the business
* Disruption to services which could lead to a breach of a legal or regulatory obligation.

This policy sets out [company]’s approach for meeting the above requirements.

|  |
| --- |
| Scope |

The information covered by this policy includes all written and electronic information held, used or transmitted by or on behalf of [company], in whatever media. This includes information held on computer systems, hand-held devices, phones and paper records.

The information covered by this policy includes:

* personal information relating to staff, clients, suppliers.
* other business information; and
* confidential information.

Information Security is everyone’s responsibility, so this Policy applies to all staff, including employees, self-employed planners, contractors, interns, volunteers and apprentices. In addition, where appropriate, the requirements of this Policy should be communicated to all third parties who are or will be processing information on our behalf, so they can ensure that their systems and controls reflect the minimum standards set out in this Policy.

This policy supplements our Data Protection and Privacy Policy as well as other policies and privacy notices in relation to information security. The contents of those policies must be considered along with the contents of this policy.

|  |
| --- |
| Risk Appetite Alignment |

The nature of information and cyber security risks is such that they can never be fully mitigated. However, the Boards have no appetite for unauthorised or unlawful processing of data and no appetite for accidental loss, destruction or damage to information held by [company] or our third parties.

|  |
| --- |
| MANDATORY REQUIREMENTS |
| Roles & Responsibilities |

**All Staff (including line managers) are responsible for:**

* Understanding their responsibilities for preventing information loss or security breaches (see section B.2).
* Undertaking regular training on information and cyber security in accordance with their annual training plan.
* Reporting any known or suspected breaches of this policy using the Risk Event Management process or, where appropriate, in accordance with our Whistleblowing Policy.
* Line managers must ensure their team members are aware of their responsibilities within this policy.

**[company] Property Management are responsible for:**

* Ensuring procedures are in place to record appropriate access to [company] offices and to provide training and information onsite to ensure the processes are followed. To provide a facility to dispose of any confidential paper waste and to retain evidence of the secure disposal.

**The Group Executive and Boards are responsible for:**

* Ensuring that the business is appropriately resourced to implement the minimum standard as set out in this policy.

**The Group Risk Committee is responsible for:**

* Reviewing the effectiveness of arrangements in place to identify, manage and mitigate information and cyber security risks.
* Reviewing and challenging reports on information security breaches and proposed actions to address these breaches and to prevent recurrence.

**Director of Technology, assisted by the** **[company] Technology team is responsible for:**

* Ensuring that a robust and well documented information and cyber security risk management framework is in place and operating effectively.
* Maintaining, reviewing and updating this policy, in respect of changes in regulation and/ or business practice.
* Ensuring adequate controls are in place to mitigate information and cyber security risk.
* Ensuring that appropriate ongoing training is provided to all staff to ensure that they are aware of the risks and understand their responsibilities about information security.
* Providing the Group Executive and Boards with regular information and cyber security risk reporting and insights, including analysis risk exposures, control effectiveness, industry insights, etc.
* Ensuring that Information Security roles and responsibilities are clearly define and allocated.

**Third Parties**

* Third Parties should adhere to the appropriate measures designed to meet the objectives of the cyber security program and cyber risk management framework.
* Suppliers and Third Parties should be able to produce documentation or commit to routine assessments to confirm they are compliant with a suitable cyber security program.
* Suppliers and Third Parties should ensure adequate cyber security training is in place for their personnel to meet the minimum standards set out in this Policy.

|  |
| --- |
| Policy Application |

**B2.1 Management and Organisation**

Management and organisation of data is key to information and cyber security, it is essential that data is managed consistent with the [company] Information Security Policy to protect confidentiality, and integrity and to maintain its availability.

The [company] Technology team will maintain a register of its critical information assets and undertake an annual threat assessment to ensure that threats to these assets are identified, assessed, managed and controlled.

The Director of Technology will ensure that Information Security roles and responsibilities are clearly defined and allocated.

The Director of Technology, supported by the [company] Technology team is required to regularly review and report to the Group Risk Committee on [company] information and cyber security risks, the adequacy and effectiveness of existing controls, and the timely completion of actions to further mitigate these risks.

**B2.2 Physical Security**

Physical Security is a main component of information and cyber security ensuring the access to physical assets and associated facilities is limited to authorised users, devices and processes.

The [company] Technology team will ensure that adequate security is in place to restrict access to information assets, equipment and prevent unauthorised physical access, damage and interference with confidential information.

**B2.21 Clear Desk Policy**

All members of staff are required to keep a clear desk at the end of the day and maintain secure storage arrangements to protect records and equipment to prevent loss, damage, theft or compromise of confidential information.

All members of staff are required to ensure all personal data and confidential company information and equipment is securely disposed of when no longer required, including obtaining evidence of secure destruction where appropriate.

**B2.3 IT and Network Security**

Technology solutions are in place and managed in the following areas to ensure the security and resilience of systems and assets is consistent with the related policies and procedures.

Asset Management – The [company] Technology team are required to identify, document and classify its hardware and software assets and assign ownership of protection responsibilities.

Home and Mobile Working – The [company] Technology team are required to ensure adequate security is in place to support mobile working and the use of mobile devices, e.g., laptops, mobile phones. This will include endpoint configuration and firewall management to guard against unauthorised connections.

Secure Configuration – The [company] Technology team are required to configure new and existing hardware to reduce vulnerabilities and provide only the functionality and services required.

Removable Media – The [company] Technology team are required to establish controls to manage the use of removable media to prevent unauthorised disclosure, modification, removal or destruction of personal data or confidential company information.

System Password Security – The [company] Technology team are required to set out appropriate password security procedures and rules for information systems and to establish a process to detect any unauthorised access or anomalous use. As demonstrated in the password safety eLearning module in the [company] Learning Management System.

Malware Protection – The [company] Technology team are required to establish effective anti-malware defenses to protect assets from malware infection.

Backup and Restoration – The [company] Technology team are required to routinely back up electronic information to help restore information in the event of business disruption.

Monitoring – The [company] Technology team are required to log and monitor user and system activity to identify and help prevent and minimise the impact of any unauthorised access or activity and help prevent data breaches or loss of confidential company information.

Patch Management – The [company] Technology team are required to maintain a patching strategy to ensure the appropriate testing and deployment of the latest security patches to prevent the exploitation of technical vulnerabilities whilst maintaining availability.

Perimeter Defenses – The [company] Technology team are required to have in place appropriate tools and techniques to protect IT systems from external attack and exploitation and prevent data breaches and loss of confidential company information and undertake regular testing of these defenses.

**B2.4 Access Control**

Access Control is essential to information and cyber security to ensure that access to information and assets is limited only to authorised users, devices and processes. Access Control will also ensure that access and permissions levels are managed, verified and revoked as necessary as the access requirements change.

The [company] Technology team will ensure suitable controls are in place and managed so that only those colleagues with appropriate permissions can access and when accessing information and systems they are authorised to do so, as set out in the User Access Management Policy.

**B2.5 Sharing of information outside of [company]**

Personal data or confidential company information may only be shared with third parties where they have a legitimate interest in and basis for having access to that information. In such circumstances the contract owner or supplier relationship manager within [company]:

* Will communicate the requirements of this Policy to the third parties so they can ensure that their systems and controls meet the minimum standards set out in this Policy.
* Will use this Policy, the Data Privacy Policy and supporting documents as the basis for due diligence of such third parties.
* Will ensure all such arrangements adhere to the Procurement & Outsourcing Policy and Third-Party Management Framework
* Will gain the approval of the [company] contract owner or relationship manager before any personal data or confidential company data is shared under such an arrangement.

A client’s personal data may be included in communications with them specifically or a third party where the written authority of the client has first been obtained, for example, provision of information to a client’s accountant. Any such communication must be appropriately secured whilst in transit, for example, if sending via email, this must be encrypted.

Under no other circumstances should any personal data or confidential company information be shared outside of [company]’s network or devices or authorised third parties without appropriate permissions having been obtained.

Furthermore, under no circumstances should client data be downloaded to personal devices such as USB storage devices, mobile phones or emailed to personal email addresses, or discussed in a public setting where sensitive information could be disclosed to those who should not have access to it.

**B2.6 Training and Awareness**

Information security training is provided through the [company] Learning Management System and must be completed by everyone, regardless of their role in [company].

* In certain cases, additional modules may be assigned dependent on the role as part of tailored training.
* E-learning modules will be supplemented with face-to-face focused training as and when required.

It is the responsibility of all line managers to ensure that their staff are trained to carry out their role in a way that is compliant with current information security regulations. If following completion of the above training provided by [company], you require further tailored training, this should initially be raised by your line manager, who will either provide further guidance, or raise the training need with learning and development and the DPO or Director of Technology.

* Additional training on day-to-day processes should be carried out by line managers prior to the individual commencing their role, and there on, periodically when a need arises.

**B2.7** **Incident Management**

Unfortunately, cyber-attacks and data breaches may still occur and, if they do, it is important that [company] is able to respond effectively and efficiently to minimise the impact. Therefore, the [company] Technology team will develop and regularly test a cyber response plan and a critical incident plan involving all relevant stakeholders.

|  |
| --- |
| Monitoring, Testing, Reporting, and Measurement of Effectiveness |

Assurance activity will be undertaken by Risk & Compliance and /or by appropriately qualified third parties. The results of assurance activities will be shared with the Executive and, where appropriate, Boards and the Group Risk Committee.

Effectiveness will be measured through:

* Regular first line monitoring of adherence to the Policy and Framework.
* Regular review of MI by the Boards, Executive Committee, and Group Risk committee.
* The review of any risk events, service and performance issues in relation to information security arrangements by the Group Risk Committee and other relevant forums will be used to consider any changes to the controls, Policy and/or Framework.
* Ensuring a continuous yearly Cyber Essentials accreditation to maintain and improve cyber security encompassing infrastructure, systems and remote working to mitigate the risk from common cyber threats

|  |
| --- |
| Breaches |

Any Breach of this policy will be treated as serious and may result in disciplinary action. Breaches of the policy must be reported in accordance with the Risk Event reporting process.

|  |
| --- |
| Next Review Date |

This policy will be subject to annual review. The next review will be in June 2023.

|  |
| --- |
| CONTACT FOR QUERIES AND GUIDANCE ABOUT THIS POLICY |

Queries to be initially addressed to the IT Service Operations team.

|  |
| --- |
| SUPPORTING & REFERENCE MATERIALS |
| * IT Security Framework * ISMS Planner * Data Privacy and Protection Policy * Mobile Device Acceptable Use Policy * Acceptable Use Policy * Remote Working Policy * Corporate Email Usage Policy * Internet Usage Policy * Employee Confidentiality Policy * Procurement & Outsourcing Policy and Third-Party Management Framework * ROPA * Cyber Essentials * IT Incident Management Process |

# REVIEW AND APPROVAL OF POLICY

|  |  |  |
| --- | --- | --- |
| **Reviewed by** | **Job Title/Role** | **Date** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **Approved by** | **Job Title/Role** | **Approval Date** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| HISTORY AND VERSION CONTROL | | | |
| **Version #** | **Author** | **Comments** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |