POLICY EXCEPTION Risk/Issue acceptance Request

Requestor to populate	**Policy/Key Risk** (Include Link where applicable)	**AI (Artificial Intelligence) Policy/Data Security Key Risk** Global Artificial Intelligence Policy (sharepoint.com) Global Information Security Policy v1.1 Approved.pdf		
	Policy and or Key Risk requiring exception	**AI Policy Extract:** 5.4 Software as a Service solutions, open-source libraries and public web services will require documentation or evidence that appropriate data segregation rules are in place and that FSI data is not used to train or improve their core models. **Global Information Security – Data Classification and Handling (DCH) Policy Extract:** Purpose: The purpose of the Data Classification & Handling (DCH) policy is to ensure that information and technology assets are properly classified, and measures are implemented to protect First Sentier Investors' data from unauthorised disclosure, regardless of whether it is being transmitted or stored. Applicable statutory, regulatory, and contractual compliance obligations dictate the safeguards that must be in place to protect the confidentiality, integrity, and availability of data.		
	Date of exception request			
	Requestor Name			
	Requesting Business Area / Project			
	ELT (Executive Leadership Team) Owner accepting the risk			
	Rationale for Acceptance			
	Risk Appetite Correlation and Tolerance Rating	**Information Security - Very Low** **Data Management - Low**		
	Residual Risk Rating (using 5x5 risk matrix)	**Residual Likelihood**	**Residual Impact**	**Aggregate Rating**
	Risk Assessment			
	Risk(s) or Issue to be accepted (Dependent whether within or out of appetite)			
	Agreed mitigating controls			
Assessor to Populate	**Assessor Name**	AIG (AI Governance) Group		
	Assessment Date			
	Maximum Period of acceptance granted (Not exceeding a 12-month period)	Exceptions must be reviewed annually and may need to be re-risk assessed where any fundamental changes have been made.		

	Expiry / Review Date	At a minimum, the exception should be reviewed and re-assessed from a risk perspective annually– re-assessment due 12 months from approval date
	Request and Recommendation:	1. Accepting Exco member to provide written confirmation that they accept the risk described within this document 2. The exception is recorded on Riskonnect and scheduled for review in 12 months.
	Consulted Parties:	AIG Group – inclusive of IT, GIS, Data Management, Risk Compliance, and relevant AI SME representation.

Please proceed to the next section if you are seeking to you risk accepting access to AI Systems or Products.

AI Risk Assessment Form

This form should be used to determine the level of risk in using a specific AI System or product. The assessment will determine the oversight and controls required unless the AI System must be treated as High Risk because of regulatory requirements. See the AI policy [LINK] for regulatory definitions.

Please note - This assessment does not replace the Strategic Sourcing, Technology or Data assessments that may be required.

Measure	Low	Moderate	High	Very High	Result e.g Low
Criticality	Used only for information purposes, may influence negligible/minimal risk internal decisions	Relied upon within the business as an informative resource, decisions are part of an important internal service	Relied upon internally, impacts high risk decision making, which could have a downstream impact on clients	Critical to High-Risk internal decision making and/or direct link to influencing or guiding client decision making	Low
Audience	Localised, used, or viewed by a team or department	Senior Management, Decision Forums, Business Partners, Regional/Global reach	Executive Leaders, Regional, Global reach, could impact client decision making	Board, Global reach, significant population of clients, Regulator, external stakeholders	Low
Data Privacy (The risk and impact of creating bias where AI misinterprets data increases in line with the privacy materiality range**)	Data is not commercially sensitive and/or related to persons living or deceased	Data has been anonymised, pseudonymised	Data such as Proprietary information, including financial and PII relating to clients and/or employees	Sensitive PII data e.g., medical, religious, sexual orientation, etc	Low
Ethical use	AI system is not used in a way that could create bias, discrimination, or	AI system could create bias or ethical issues, but the training data is	AI system could create bias or ethical issues and	AI system could create bias or ethical issues and requires oversight.	Low

	other ethical impacts	diverse, build and testing mitigates this issue and controls are in place	requires oversight.		
Data Classification (Link to Data Classification Standard)	External	External, Internal	Internal, Confidential	Confidential	Low
Complexity and interpretability	Straightforward and can be understood by non-subject matter expert (SME) in AI and/or the process	Moderately complex may have interdependencies, can be interpreted by a skilled person or SME in AI and/or the process	Has several interdependencies and a level of complexity that requires specialist or niche knowledge of the workings of AI and/or the process	May be linked to key business procedure and complex applications that require specialist developer knowledge or maintenance	Mod
Cybersecurity (Vendor Assessment)	Cybersecurity Assessment Framework (CAF) (or regional equivalent) is assessed as **Achieved**	Cybersecurity Assessment Framework (CAF) (or regional equivalent) is assessed as **Partially Achieved**	Cybersecurity Assessment Framework (CAF) (or regional equivalent) is assessed as **Partially Achieved**	Cybersecurity Assessment Framework (CAF) (or regional equivalent) is assessed as **Not Achieved**	Low
Potential impact of failure (financial)	Minor	Moderate	Major	Severe	Low
Potential impact of failure (non-financial)	Minor	Moderate	Major	Severe	Low
Sustainability impact	AI system provider adheres to sustainable and ethical practices	AI system provider adheres to some sustainable and ethical practices	AI system provider does not detail their approach to sustainable and ethical practices	AI system provider does not have an approach to sustainable and ethical practices	Low
Availability/ Resilience	Can be maintained, repaired by internal onsite team or users. A breakdown or failure would be easily detected and could be	Maintenance and repair can be achieved by a member of staff with specific skills. A breakdown or failure may not be immediately identifiable and	Specialised external and/or vendor support is required to maintain and repair. Thorough/ multitiered validation controls	Niche specialised developer or, vendor support to maintain and repair. Specialist/niche validation required to detect any anomalies or deviations.	Low

	rectified with relative ease quickly.	would require output validation	are required to detect any anomalies or deviations.		
Action – AI or Human execution	Human executed (Human in the Loop)	Human executed (Human in the Loop)	AI execution (Human on the Loop)	AI execution (sampled oversight)	Low

*The impact of data being misinterpreted by AI increases in line with the privacy materiality range e.g. Low – Public data risk of bias and potential impact is low – Very high the risk and impact are very high.

Definitions:
Criticality – Refers to the impact that an event, process, or system failure due to this AI system, would have on the organisation's ability to achieve its objectives.
Audience – Refers to the reach the application output and influence it is likely to have.
Data Privacy – Provides guidelines on different risk levels depending on the data type.
Ethical Use – refers to the way that the AI system is used and whether that could create bias or other ethical issues.
Data Classification – what type of data is consumed by the application aligned to FSI Data Classification Standard.
Complexity and interpretability – refers to how easy or difficult it is to understand how the AI works, is trained and the data used to train.
Cybersecurity (AI Vendor Assessment) - The outcome of the Cybersecurity assessment available here [LINK]
Potential Impact and probability of failure – financial; based on the Risk Management Framework (RMF) impact matrix If the application does not work as intended, what is the maximum financial impact the organisation might face in terms of repairs, upgrades, reporting, compensation, etc.
Potential Impact and probability of failure – non-financial - for all other measures captured within the RMF impact matrix what would be the maximum perceived impact from the perspective of, Clients, Regulators, reputational, etc.
Sustainability impact – refers to the impact of the AI system in terms of energy usage, consumption, carbon, and other sustainability factors.
Availability/Resilience – Consider factors such as operational soundness how likely is it to break down and how often relative with the complexity and the availability of skilled individuals, vendors etc. to support maintenance and repair.
Action – AI or Human execution - Human executed / Human in the Loop = An employee reviews the AI generated outcome and underlying data to validate the AI's output, applying the contextual judgement/review that may be missed by the AI system. The employee completes any decision making and communication of the outcome.
AI execution = The process completes without any human/employee intervention or effort. These outcomes can be reviewed retrospectively, which could include sampling or reviewed at the model level, usually both