Bank of Ireland Group Third Party Policies

November 2024

Bank of Ireland

Bank of Ireland Group Third Party Policies

At Bank of Ireland Group ("the Group"), our relationships with our third-party suppliers and partners underpin our strategy to deliver stronger relationships with customers and colleagues, and a simpler, more efficient, and sustainable business.

Group Third-Party Policies summarise internal Group Policy statements into mandatory clear requirements that we expect our Third-Party Suppliers to meet and reflect our commitment to regulatory compliance, operational resilience, operational excellence, and our shared success. Environmental, Social and Governance (ESG) factors, including relating to climate change, and ethical, transparent, and sustainable use of Artificial Intelligence should also be assessed and addressed by suppliers in meeting the requirements set out in this document.

Group Third Party Policies complement the Group Supplier Code of Supplier Responsibility which sets out the key social, ethical and sustainability standards that we want our suppliers to achieve, aligned with our Sustainability Strategy and with the Group Code of Conduct.

Group Third-Party Policies and Code of Supplier Responsibility are key components of the Group's use of the Financial Supplier Qualification System (FSQS) on-line portal for suppliers to submit relevant business and compliance information about your organisation. Suppliers are requested confirm your agreement to comply with Group Third Party Policies and the Code when you complete our Financial Services Qualification System (FSQS) process.

The Code of Supplier Responsibility and further detail on FSQS can be found in the Working with Suppliers section of www.bankofireland.com.

If you are unclear on anything in this document, please contact your Group Relationship Manager for clarification.

If there is any inconsistency between this document and the terms of your third-party supplier agreement with the Group, the order of priority for the purpose of construction of agreed terms will be that your third-party supplier agreement takes precedence over this document.

Scope

All Group third party suppliers are expected to comply with Group policy compliance obligations as more fully set out in their contractual arrangements with the Group together with the minimum expectations and requirements under each policy area as set out in this document.

A 'supplier' is defined as a person or company that falls in to one or more of the following categories:

- A third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.
- A third-party entity that provides the Group directly or indirectly with a product or service for the Group's use on a continuing basis.
- A third-party entity that uses the Group's brand under licence to provide a product or service directly or indirectly to customers of the Group.

What You Need to Do

As a third-party supplier, you are expected to:

- confirm your agreement to comply with Group Third Party Policies and Group Supplier Code of Responsibility (and any future revisions) when you complete our Financial Services Qualification System (FSQS) process.
- Provide details of your organisation's policies and controls when you complete our FSQS process.
- Explain the principles and expectations of Group Third Party Policies to your officers, employees and sub-contractors that support services to the Group or work on Group projects.
- Inform the Group if anything changes and you are unable to comply with the expectations and standards set out in in this document and your contractual obligations to the Group.

What we expect of you

For the purposes of this document, Group minimum requirements of our Third-Party Suppliers are grouped into thirteen risk areas.

1. Customer Protection
2. Operational and Regulatory Risk
3. Business Continuity Management & Operational Resilience
4. Information & Cyber Security
5. Data Protection and Privacy
6. Fraud, Anti-Bribery & Corruption
7. People and Pre-employment Screening
8. Third Party Risk Management & Outsourcing
9. Transaction Processing
10. Information Technology
11. Physical Security
12. Data Governance
13. Model Risk Management

In each case listed on the following pages, for the purpose of this document we describe our minimum expectations using the term '**we expect.**'
In some areas, we aspire to meet certain standards, and in these cases, we use the term **'we encourage.'**

If you are unclear on anything relating to these requirements or how they interact with your contractual obligations to the Group, please contact your Group Relationship Manager for clarification.

How to Speak Up

The Group is committed to conducting our business with honesty and integrity and we expect everyone working on behalf of the Group to maintain these high standards.

The Group Speak Up Policy explains what a Speak Up concern is and makes it easier for colleagues, including suppliers, to safely and confidentially raise a Speak Up concern about suspected or actual wrongdoing in a work-related context, without fear of penalisation.

The Group Speak Up Policy is available via Corporate Governance – Bank of Ireland Group Website and contains all the relevant contact details and information on resources/supports to help you raise a Speak Up concern.

1. Customer Protection Requirements

We expect all our suppliers who have contact with Group customers to effectively manage conduct risk in support of fair outcomes for Group customers.

We **expect** you to:

- Have an up-to-date customer protection policy.
- Ensure all employees receive an appropriate level of customer protection training.
- Operate clear customer engagement and communication procedures which focus on customer needs, and which address as applicable, product and/or service design, sales and distribution, customer servicing, complaint handling, rectification, and communications that may be required to meet legal or regulatory requirements.
- Operate product lifecycle reviews to ensure the product and/or service remains appropriate for customers and continues to deliver fair outcomes.
- Operate customer complaints procedures to include complaints identification, recording, remediation, escalation, and reporting activities.
- Operate procedures to identify, assess, record, and support vulnerable customers.
- Observe proper standards of market conduct.
- Ensure all staff receive and continue to receive an appropriate level of customer treatment training.

2. Operational and Regulatory Risk Requirements

We expect all our suppliers to effectively manage their operational and regulatory risks and to comply with relevant regulatory requirements for the services provided.

We **expect** you to:

- Operate a Risk Management Framework to identify, assess, measure, and mitigate operational risks.
- Have an up-to-date Risk Management Policy.
- Ensure all employees receive an appropriate level of Operational and Regulatory risk training.
- Proactively identify and manage operational and regulatory risks.
- Have in place a formal assessment of exposures to those risks.
- Have in place ongoing monitoring of risks and associated controls.
- Implement measures to avoid, mitigate, or transfer financial or other negative impacts, were these risks to materialise.
- Operate a governance structure to report on risk management activities and events to the Group.
- Maintain adequate insurance to cover operational risks.
- Identify and notify the Group of any operational risk or regulatory risk events relevant to the services to the Group.

We **encourage** you to:

- Be certified (or working towards certification) to ISO 31000, the internationally recognised Risk Management Standard.

3. Business Continuity Management & Operational Resilience Requirements

We expect all our suppliers to ensure the continuity of our services from potential disruption events. This includes but is not limited to interruption to services through the loss of key personnel, widespread loss of staff, loss of premises, loss of sub-contractors, data centre disruptions, cyber incidents, geographical events, socio-political events, and pandemics.

We **expect** you to:

- Have an up-to-date Business Continuity Management (BCM) Policy including IT Service Continuity requirements.
- Ensure all employees receive an appropriate level of BCM training.
- Ensure that adequate risk identification and controls are in place to mitigate potential disruption events originating from both internal and external threats.
- Have up to date and tested continuity, response, and recovery plans to respond to disruption events including crisis and incident management.
- Have up to date and tested IT Service Continuity Management (ITSCM) Plan / Disaster Recovery Plans.
- Jointly agree a service focused Business Impact Analysis and/or impact tolerance with the Group with Recovery Time Objectives and Recovery Point Objectives documented for each service provided to the Group. These must include clear timeframes which are validated and tested on an agreed frequency.
- Document a Business Continuity Plan relevant to the services / products provided to the Group, including specific loss disruption scenarios to address technology/IT, Management of 4th and 5th party providers to the Group, People and Property.
- Schedule testing of Business Continuity Plans, ITSCM and Disaster Recovery on a regular basis and share the results of those tests.
- Provide immediate communication to your Group Relationship Manager in the event of potential and actual disruptions to Group services.
- Ensure that all requirements placed upon your third-party supplier to the Group are also extended and managed in relation to sub-contracting of the services.
- Work with the Group to develop an appropriate 'Unplanned Exit' response if requested.
- Work with the Group in support of Group supplier due diligence activities.

We **encourage** you to

- Be certified (or working towards certification) to ISO 22301, the internationally recognised Business Continuity Management Standard and/or adhere to industry best practice.

4. Information Security & Cyber Risk Requirements

We expect all our suppliers to ensure that they protect the confidentiality, integrity and availability of all Group information and information systems that they have access to. This includes protection from threats from unauthorised / accidental disclosure, corruption, unauthorised modification, loss, theft, deletion, or unavailability of information assets for legitimate business use.

These threats affect information in all formats and the supporting information systems (containers) such as infrastructure, networks, hardware, software, filing cabinets and data storage devices.

We **expect** you to:

- Have an up-to-date Information Security/Cyber Security Risk Policy.
- Ensure all employees receive an appropriate level of Information Security training.
- Implement processes, procedures, and safeguards to ensure the protection of the confidentiality, integrity, and availability of all Group Information Assets, during all stages of the information lifecycle – creation, storage, processing, transmission, and destruction.
- Ensure that adequate People, Process and Technology controls are in place to mitigate Information Security and Cyber Risk originating from both internal and external threats.
- Ensure clearly defined Employee and third-party roles and responsibilities for information security and cyber risk management are in place.
- Ensure that you operate appropriate mechanisms for responding to Information Security incidents.
- Ensure that Information Security controls are applied to all information systems and cloud services that are used to store, process, or transmit Group information.
- Ensure that adequate Information Security incident response plans and procedures are in place and tested for IS incidents such as breach scenarios which are also linked to suitable Disaster Recovery, Business Continuity and Event Management plans and procedures.
- Notify Group within an agreed timeframe of Information Security incidents affecting Group data or systems used to host or transfer this data.
- Complete and return the Group IT Security Review questionnaire when requested.

We **encourage** you to:

- Engage external independent auditors to conduct an annual audit of your information security policy, protocols, and practices.
- Be certified (or working towards certification) to ISO 27001, the internationally recognised Information Security Standard.

5. Data Protection and Privacy Requirements

We expect all suppliers who process personal data on behalf of the Group to comply with all Data Protection & Privacy obligations and legislative requirements, including having mechanisms in place to ensure the privacy rights of the individuals who are subject to the Data Processing activities are protected and always upheld. This includes all Group customers, potential customers, employees, and any other individuals for whom you process Personal Data.

We **expect** you to:

- Have a Data Protection & Privacy policy in place, supported by procedures and controls to protect Personal Data and the privacy rights of individuals, and monitor such controls to ensure they remain effective.
- Ensure all employees receive an appropriate level of Data Protection and Privacy training.
- Process Personal Data on behalf of the Bank, in line with the principles of Data Protection in addition to your contractual obligations including ensuring Personal Data is:
    - Processed lawfully, fairly and in a transparent manner.
    - Collected for specified, explicit and legitimate purposes and not further processed in ways that are incompatible with those purposes.
    - Processed with the minimum amount of personal data required to execute the task.
    - Kept accurate and up to date.
    - Only retained for as long as required to support Group business processes and regulatory obligations. In line with your contract with us, upon its termination and/or as requested by us, any personal data must be returned or permanently erased.
    - Processed in a safe and secure manner, preventing unauthorised and/or accidental access, loss, disclosure and/or alteration of such data.
- Be accountable and provide evidence of compliance with your Data Protection and Privacy obligations when requested by the Bank including.
- Have processes in place to assess and mitigate any risk to the Personal Data being processed on behalf the Group including conducting risk assessments and Data Protection Impact Assessments as appropriate.
- Have processes in place to identify and notify the Group of any Data Protection breaches, without undue delay and in line with your contractual agreements and regulatory requirements.
- Have processes in place to assist in fulfilling requests received by individuals exercising their privacy rights in line with timeframes stipulated by Group and/or regulation.
- Ensure Group personal data is not transferred to another country without prior written consent from us and ensure third parties are not appointed to process Group personal data without prior written consent from us.
- Maintain a record of all Group processing activities containing personal data as stipulated in data protection legislation.

6. Fraud, Anti-Bribery & Corruption Requirements

We expect all our third-party suppliers to ensure integrity and honesty in their dealings.

We **expect** you to:

- Have a Fraud and Anti-Bribery Policy and corruption policy.
- Ensure all employees receive an appropriate level of fraud, anti-bribery, and corruption training.
- Provide timely communication in the event of any breaches to your policy.
- Not make, authorise, seek, or accept any kind of offer, gift, kickback, illicit payment, or facilitation payment to get or keep an unfair advantage. This does not need to have to involve money.
- Not directly or indirectly (via any third party such as consultants, contractors, agents, sponsors or joint venture partners, advisors, customers, or suppliers.) offer, promise or give something intending to influence someone's behaviour or actions.
- Not use Group funds for any unlawful, improper, or unethical purpose.
- Take care when you are dealing with government or public officials as laws are strict and your actions could be misinterpreted. Never offer, promise, or give anything of value with the aim of influencing any government or public official in their work. This includes facilitation payments or "grease payments" such as payments to speed up the performance of routine governmental actions.
- Not offer or accept gifts, payment, or hospitality to encourage or reward a decision.
- Not use charitable donations or sponsorship as a way of concealing a bribe.
- Maintain a gifts and hospitality policy which makes it clear what is and is not appropriate.
- Comply with legal restrictions relating to the financing of trade, including country sanctions/trade embargoes.
- Ensure not to employ or do business with any individuals, entities or third-party suppliers that are the subject of sanctions within the relevant local jurisdiction or where to do so would constitute a breach of the regulations in that jurisdiction.

We **encourage** you to:

- Be certified (or working towards certification) to ISO 37001, the internationally recognised Anti-Bribery Standard.

7. People and Pre-Employment Screening Requirements

We expect all our suppliers to have appropriate people risk management and pre-employment screening standards.

We **expect** you to:

- Have a suitable People Risk policy in place, supported by procedures and controls to attract and maintain an employee base with the skills, capabilities, and culture necessary to execute business objectives, and adhere to employment and health and safety legislation. Policy should include hiring, diversity, and Pre-Employment Screening (PES) requirements.
- Ensure all employees receive an appropriate level of PES training.
- Provide timely communication in the event of any breaches to your policy.
- Ensure all employees are aware of and compliant with the Groups Health and Safety procedures.
- Ensure all employees are aware of the Groups Code of Conduct.
- Operate processes and controls for identification, disclosure, recording and managing conflict of interest.
- Discuss any identified conflict of interest that could impact the Group with your Supplier relationship manager in the Group.
- Maintain a list of all personnel assigned solely to work on the Group account, which must be available for inspection
- Retain a record of screening verification for all personnel working on the Group account, which must be available for inspection.

The following are the minimum standards your policy and process should cover relating to employee screening:

- **Government Issues Identification Verification**: Verify the authenticity of government issued identification documents such as a passport, drivers' licence, or national identification card.
- **Education Verification**: Validate academic qualification and certifications claimed by the individual.
- **Previous Employment Verification**: Confirm the individual's employment history, including positions held, tenure and reason for leaving past jobs.
- **Reference Checks**: Checks on previous employer references or professional references.
- **Background Checks**:
    - Credit checks for positions
    - Criminal background checks (where permissible)
    - International Background Checks: If the candidate has lived or worked abroad, on a risk based approach, checks against international databases or watchlists.

8. Third Party Risk Management and Outsourcing Requirements

We expect all our suppliers to support Group supplier due diligence activities, and to ensure, when using third parties (sub-contractors) to fulfil all or part of the contracted services, that the standards operated by the third party (referred to as Group fourth parties) are of an equal standard to those required by the Group.
The expectations here are in addition to requirements to manage your own supply chain, including Group fourth parties in a responsible manner as set out in the Group Code of Supplier Responsibility.

We **expect** you to:

- Join FSQS (Financial Services Qualification System) operated by Hellios and fully complete the FSQS questionnaire annually.
- Comply with the Group Code of Supplier Responsibility located here: Working with Suppliers | Bank of Ireland
- Support Group compliance with relevant jurisdictional regulatory and legislative requirements relating to third party and outsourcing risk management on an ongoing basis.
- Support Group supplier governance & oversight requirements including provision of information that supports supplier due diligence, audit and assurance activity and operational resilience.
- Have an agreed Business Continuity Management Plan and Exit Plan for the services provided to the Group when required by the Group.
- Implement appropriate measures to secure and protect the Group activities, services, and data against unwarranted disclosure.
- Manage Group fourth party and supply chain risk in accordance with the following minimum standards:
    - Have an up to date Third Party Risk Management Policy and process, and an appropriate organisational structure and controls to monitor and manage material Group fourth parties.
    - Complete appropriate criticality risk and impact assessments, and onboarding and ongoing supplier due diligence on Group fourth parties, including assessments of Group fourth party supplier operational capability and financial stability.
    - Complete ongoing supplier governance, oversight, and assurance on Group fourth parties including supplier performance management and contract obligations management.
    - Ensure contractual arrangements with Group fourth parties allow the Group to comply with Group legal and regulatory requirements including as relates to Group (and regulatory authorities) access, audit, and inspection rights.
    - Ensure all employees receive an appropriate level of third party risk management training.
    - Obtain Group consent prior to sub-contracting any material element of the services contracted with the Group.
    - Notify the Group immediately of any material changes to the services or sub-contracted services provided, including changes to the location from which the services or sub-contracted services are provided.
    - Notify the Group promptly of material risks or issues or events identified in relation to your service and /or any suppliers or sub-contractors involved in the provision of services to the Group.
    - Ensure appropriate contingency, business continuity and exit plans are in place for Group fourth parties.

9. Transaction Processing Risk Requirements

We expect all our suppliers providing payment transaction processing services to Group to ensure that Group payments are processed in a timely and correct manner and in line with all regulatory and scheme requirements.

Payment processing services includes any activities involved in any part of the Payment processing cycle for Group payments such as initiation, receipt, validation, acceptance, processing, settlement, reconciliations, or exceptions management.
For the avoidance of doubt, the following relationships are not deemed to be in the provision of payment processing services to Group and are therefore outside of the scope of the below requirements:

(1) Correspondent Banks
(2) Parties who have entered into Joint Venture agreements with the Group.

We **expect** you to:

- Have an up to date Transaction/payments processing policy.
- Ensure all staff receive and continue to receive an appropriate level of transaction /payments processing training.
- Process all Group customer payment instructions in line with the customer instruction, without any information amended, deleted, or omitted.
- Verify that all payment instructions received are from the customer and that prior to processing the instruction, ensure that it is in line with the rules of the account (e.g., per account mandate, signing rules) and approved procedures.
- Ensure segregation of duties is in place for the input and authorisation of Group payment instructions and that staff involved in these activities are also not involved in the reconciliation activities on the relevant accounts
- Document Payment processing approval limits enforced with manual or automated controls
- Document payment processes which are subject to periodic review. The frequency of review must be derived from the criticality of the procedures and be clearly documented.
- Adhere to the relevant Channel or System Policy where it is used in support of your payment processing activity.
- Have a documented process in place to handle events where automated payment processing is interrupted and manual intervention is required. This process should ensure that there is management sign off for the actions taken; a four eyed check of the actions; and an audit trail retained of the actions taken.
- Notify and engage with Group immediately on any incidents where payment processing for Group payments has been disrupted.

10. Information Technology Requirements

We expect all our suppliers to effectively manage their Information Technology risks as they apply to hosted, managed, or outsourced services to the Group. The listing below sets out at a high level the key IT Risk areas of focus that apply to some or all third-party services, including Cloud Services being provided to the Group.

We **expect** you to:

- Have an Information Technology Risk policy.
- Ensure all employees receive an appropriate level of Information Technology risk training.
- Ensure all Information Technology changes to services supporting the Group are progressed according to a documented service introduction, transition, and deployment framework.
- Have documented event, incident, escalation, and problem management processes including roles and responsibilities for different incident scenarios to identify, categorise and appropriately manage and track incidents and problems through to closure including completion of root cause analysis and lessons learned reports in a timely manner that supports the Group in meeting regulatory reporting obligation where applicable.
- Notify and engage with Group on IT issues affecting or with the potential to disrupt Group data or systems used to host, process or transfer data.
- Notify us promptly where IT services are approaching end of life, or have a significant identified security vulnerability, so that we can collaborate on timely corrective action.
- Have an appropriate documented data archival and retrieval processes, together with robust management of archival and data restoration testing aligned to relevant BCM and recovery Service Level Agreements.
- Utilise documented processes including appropriate controls to provide monitoring of system resources with robust availability, performance, and capacity forecasting in place to minimise the risk of service disruptions.
- Maintain an asset management and configuration register/database which includes location, security classification and ownership of assets which underpin business systems which support Group services.
- Record and maintain the currency versions of all components (hardware, firmware, software) of critical services.

We **encourage** you to:

- Manage delivery of technology changes to an externally recognised framework, such as ITIL.

11. Physical Access Requirements

The following requirements apply to suppliers who have access to Group data and/or are receiving and/or distributing data to the Group.

We **expect** you to:

- Have an up-to-date Physical Access Security policy/standard.
- Ensure employees receive an appropriate level of physical access security training.
- Operate an access control system to include defined authorisation levels.
- Have defined a process for identification of and authenticating personnel and visitors.
- Operate surveillance and monitoring systems, and physical barriers at key entry points.
- Establish standards for assessing, responding to, and reporting physical access risks.

12. Data Governance Requirements

The following requirements apply to suppliers who have access to Group data and/or are receiving and/or distributing data to the Group.

We **expect** you to:

- Have an up-to-date Data Risk Management policy/standard.
- Ensure employees receive an appropriate level of data risk management training.
- Have measures/procedures to monitor, manage and where applicable remediate and improve data quality, accuracy, and consistency.
- Have measures/procedures to manage data retention and deletion in line with applicable regulations and legislation.

13. Model Risk Management Requirements

The following requirements apply to suppliers who use models in the provision of services to the Group, subject to intellectual property arrangements that may apply.
For the purpose of this policy, a "model" refers to a quantitative method, system or approach that satisfies each of the follow conditions:

- Processes inputs into one or more outputs applying theoretical and expert judgemental assumptions; using statistical, financial, or mathematical techniques
- Produces an output that is an estimate or forecast used for measurement and management purposes
- Creates output that is used to assist with decision making or to make automated decisions

We **expect** you to:

- Have an up-to-date Model Risk policy/standard.
- Ensure employees receive an appropriate level of model risk management training.
- Have defined processes for the management of model risk including relating to model development, model validation, model implementation and use, and model performance monitoring.
- Provide evidence of the monitoring and validation of the models as may reasonably be requested by the Group
- Support the Group (or any party appointed by the Group) in undertaking independent validations or reviews of the models you provide
- Provide evidence that the models you provide meet any relevant regulatory requirements including as relates to responsible and transparent use of Artificial Intelligence if applicable.

What we will do - Our commitment to you

We will commit to:

- Engage with you to support your understanding of the Group Third-Party Policies applicable to the services you are providing to Group.
- Ensure the latest Group Third-Party Policies are available in the 'Working with Suppliers' section of www.bankofireland.com and with FSQS.

Compliance with Group Third Party Policies

We expect all our suppliers to meet or exceed all the requirements in this Group Third Party Policies document.

In situations where you are not compliant with the requirements set out in this document, you must let us know. We will work with you on the development of an improvement plan.

If there is any inconsistency between this document and the terms of your third-party supplier agreement with the Bank, the order of priority for the purpose of construction will be that your third-party supplier agreement takes precedence over this document.

Useful Links

You can access more information on how we work with our Suppliers at the 'Working with Suppliers' section of **www.bankofireland.com**

We want to hear from you.

Please contact us with any feedback or questions you may have.

responsiblebusiness@boi.com

@BankofIreland

@BankofIreland