Third Party Policies

November 2020

Bank of Ireland

Third Party Policies

Bank of Ireland Third Party Policies translate Bank internal Policy statements into mandatory clear requirements that we expect our Third Party Suppliers to meet. We require our suppliers to comply with the Bank Third Party Policy statements provided in this document when applicable to the services provided to the Bank.

This approach to Third Party Policies sits alongside our membership of the Financial Supplier Qualification System (FSQS), our on-line portal for you to submit information and compliance data about your organisation. You can read more about FSQS system in the 'Working with Suppliers' section of **www.bankofireland.com**.

If you are unclear on anything in this document, then please contact your Bank of Ireland Relationship Manager for clarification.

Scope

All Bank of Ireland suppliers are expected to comply with the minimum expectations and requirements under each policy area in this document; these are in addition to the requirements in your supplier agreement(s) with Bank of Ireland, to comply with applicable laws, regulatory requirements and applicable Bank of Ireland Group policies.

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.
- Provides the Group directly or indirectly with a product or service for the Group's use on a continuing basis
- 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

You are **expected** to:

- Provide details of your own policies and compliance with Bank of Ireland expectations (and any future revisions) when you complete our FSQS process.
- Explain the principles and expectations of these Third Party Policies to your officers, employees and key sub-contractors that support Bank of Ireland or work on our projects.
- Inform us if anything changes and you are unable to comply with the expectations and standards set out in these Third Party Policies.

What we expect of you

Our minimum requirements of our suppliers are grouped into ten key areas:

1. Customer Treatment Requirements
2. Operational and Regulatory Risk Requirements
3. Business Continuity Management Requirements
4. Information Security Requirements
5. Data Protection and Privacy Requirements
6. Fraud, Anti-Bribery & Corruption Requirements
7. Pre-employment Screening Requirements
8. Sourcing and Supply Chain Management Requirements
9. Payments Processing Requirements
10. Information Technology Requirements

In each case listed on the following pages, 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'**.

Again, if you are unclear on anything relating to these requirements then please contact your Bank of Ireland Relationship Manager for clarification.

How to Speak Up

If you are concerned about any actions or decisions that contravene the expectations and standards set out in the Third Party Policies, please contact your Bank of Ireland Relationship Manager.

If you are uncomfortable doing this, please contact our confidential Speak Up mailbox at: **SpeakUp@boi.com**.

All reports are taken seriously and the identity of those who raise a concern is kept confidential.

1. Customer Treatment Requirements

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

We **expect** you to:

- Have an up to date customer treatment policy.
- Operate clear customer engagement procedures which focus on customer needs and which address as applicable, product and/or service design, sales and distribution and customer servicing, complaint handling and rectification.
- Operate customer complaints procedures to include complaints receipt, recording, assessment and resolution 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 be in compliance 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.
- Proactively identify operational 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 Bank of Ireland.
- Maintain adequate insurance to cover operational risks.
- Identify and notify the Bank of Ireland Group of any operational risk or regulatory risk events.
- Ensure all staff receive and continue to receive an appropriate level of operational and regulatory risk training.

Important Note:

- Data Protection Breaches. Data Protection related events must notified immediately on becoming aware of the Data Protection related event to facilitate further investigation by BOI and Regulator reporting timelines.
- Consumer Protection Code Breaches. (ROI only) Errors, per the Consumer Protection Code4 (CPC), must be notified as soon as identified including details of the error and cause of the error, regardless of potential or actual financial impact.

We **encourage** you to:

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

3. Business Continuity Management 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 person dependencies, widespread loss of staff, loss of premises, loss of sub-contractors, data centres disruptions, cyber incidents, geographical events, socio-political events and pandemics.

We **expect** you to:

- Have an up to date Business Continuity Policy including IT Service Continuity Management requirements / Disaster Recovery[1]. Provide training and build awareness of that policy with your staff.
- Ensure that adequate risk identification and controls are in place to mitigate potential disruption events originating from both internal and external threats.
- Have in place tested continuity, response and recovery plans to respond to disruption events including crisis and incident management.
- Have an up to date and tested IT Service Continuity Management (ITSCM) Plan / Disaster Recovery Plans.
- Jointly agree a service focussed Business Impact Analysis with the Bank of Ireland Group.
- Have Recovery Time and Recovery Point Objectives (RTO / RTP) documented for each service provided to Bank of Ireland Group. To 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 Bank of Ireland.
- Schedule testing of Business Continuity Plans, ITSCM and Disaster Recovery on a regular basis and share the results of those tests.
- Provide timely communication to your Bank of Ireland Relationship Manager or Partner Manager in the event of both potential or actual disruptions to services.
- To ensure that all requirements placed upon your third party are also extended and managed in relation to sub-contracting of the services.
- Ensure all staff receive and continue to receive an appropriate level of business continuity management risk training; including all elements of the BCM lifecycle.

We **encourage** you to:

- Be certified (or working towards certification) to ISO 22301, the internationally recognised Business Continuity Management Standard.

[1] It is acceptable for these documents to be separate rather than inclusive

4. Information Security Requirements

We expect all our suppliers to ensure that they protect the confidentiality, integrity and availability of all Bank of Ireland information and information systems that they have access to. This includes protection from threats which include 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.
- Implement processes, procedures and safeguards to ensure the protection of the confidentiality, integrity and availability of all Bank of Ireland 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 Bank of Ireland 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 Bank of Ireland within an agreed timeframe of Information Security incidents affecting Bank of Ireland data or systems used to host or transfer this data.
- Complete and return the Bank of Ireland IT Security Review questionnaire when requested.
- Ensure all staff receive and continue to receive an appropriate level of information security training.

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 227001, the internationally recognised Information Security Standard.

5. Data Protection and Privacy Requirements

We expect all suppliers who process personal data on behalf of the Bank of Ireland Group to have mechanisms in place to ensure the privacy rights of the individuals who are subject to the processing activities are protected and upheld at all times, this includes Bank of Ireland customers, potential customers, employees and any other individuals for whom Bank of Ireland process personal data.

We **expect** you to:

- Process all personal data on behalf of the Bank of Ireland, in line with the principles of data protection 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 Bank of Ireland 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, disclosure and/or alteration of such data.
- Be accountable and where requested by Bank of Ireland, provide evidence of compliance with your data protection and privacy obligations.
- Have processes in place to assess any risk to the Personal Data being processed and the Privacy Rights of individuals including conducting risk assessments and data protection impact assessments as appropriate.
- Have appropriate policies, procedures and controls in place to protect Personal Data and Privacy Rights of individuals and monitor such controls to ensure they remain effective.
- Have processes in place to identify and notify Bank of Ireland of any data protection breaches, without delay and in line with your contractual agreements.
- Have processes in place to assist in fulfilling requests received by individuals exercising their privacy rights in line with timeframes stipulated by Bank of Ireland and/or regulation.
- Ensure Bank of Ireland personal data is not transferred to another country without prior written consent from us.
- Ensure third parties are not appointed to process Bank of Ireland personal data without prior written consent from us, consult us prior to any changes with third parties who you depend on for processing the personal data and have controls in place to manage sub processors and chain outsourcing.
- Maintain a record of all Bank of Ireland processing activities containing personal data as stipulated in data protection legislation.
- Ensure all staff receive an appropriate level of data protection and privacy training.

6. Fraud, Anti-Bribery & Corruption Requirements

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

We **expect** you to:

- Have a Fraud and Anti-Bribery Policy and corruption policy.
- 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 to 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 to use BOI funds for any unlawful, improper or unethical purpose.
- To 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.
- Ensure all staff receive and continue to receive an appropriate level of fraud, anti-bribery and corruption training.

We **encourage** you to:

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

7. Pre-Employment Screening Requirements

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

We **expect** you to:

- Have a suitable Pre-Employment Screening (PES) Policy.
- Maintain a list of all personnel assigned solely to the Bank account, which must be available for inspection.
- Retain a record of screening verification for all personnel working on the Bank account, which must be available for inspection.

The following are the minimum standards required of your PES process to check:

- Official proof of identity and residential address.
- Details of relevant education and qualifications (if required for the position).
- Employment history and employment references (if required for the position).
- Declaration of any previous relevant convictions.
- Confirmation of right to work in the respective jurisdiction.

8. Sourcing and Supply Chain Management Requirements

We expect all our suppliers to ensure, that when using third parties to fulfil part of the contracted services, the standards operated by the third party are of an equal standard to those required by Bank of Ireland.

The expectations here are in addition to requirements to manage your own suppliers in a responsible manner as set out in the Group Code of Supplier Responsibility.

We **expect** you to:

- Have a Sourcing Risk Management Policy which includes the management of supply chain risk.
- Provide an Exit Plan to the Bank of Ireland Group subject to review and approval through your Relationship Manager.
- Hold scheduled governance meetings with your suppliers to review operational, commercial and risk management matters with clear minutes and actions.
- Hold regular quantitative and qualitative performance targets reviews with your suppliers.
- Monitor your supplier's adherence to contractual obligations.
- Complete a reassessment of operational and regulatory risks when a significant third party supplier change or event occurs.
- Have a process for reporting our supply chain incidents and events to Bank of Ireland.
- Have appropriate processes in place to identify, mitigate and monitor potential risks including effective controls.
- Notify the Bank of Ireland of any risks or issues identified in relation to any suppliers or sub-contractors involved in the provision of services to the Bank.
- Notify the Bank of Ireland immediately of any material changes to the services provided including the location from which the services are provided.
- Not to sub-contract any element of the services contracted with Bank of Ireland Group without prior consent.
- Ensure all staff receive and continue to receive an appropriate level of sourcing and supply chain training.

We **encourage** you to:

- Strive for a supply base that is inclusive and diverse (namely supporting SMEs, Social Enterprises as well as under-represented groups).

9. Payment Processing Requirements

We expect all our suppliers providing payment processing services to Bank of Ireland to ensure that Bank 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 BOI payments such as; initiation, receipt, validation, acceptance, processing, settlement, reconciliations or exceptions management. **NB:** for the avoidance of doubt, the following relationships are not deemed to be in the provision of payment processing services to Bank of Ireland (BOI) and are therefore outside of the scope of the below requirements:

(1) Correspondent Banks

(2) Parties who have entered into Joint Venture agreements with BOI.

We **expect** you to:

- Process all BOI 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 BOI 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 BoI immediately on any incidents where payment processing for BOI payments has been disrupted.
- Ensure all staff receive and continue to receive an appropriate level of payments processing training.

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 being provided to the Group.

We **expect** you to:

- 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 in a timely manner.
- Notify and engage with Bank of Ireland on IT issues affecting or with the potential to disrupt Bank of Ireland data or systems used to host, process or transfer data.
- 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 SLAs.
- 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.
- Ensure all staff receive and continue to receive an appropriate level of information technology risk training.

We **encourage** you to:

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

What we will do

Our commitment to you

We will commit to:

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

Compliance with Third Party Policies

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

In situations where you are not yet 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.

However, if the issue is serious enough or cannot be resolved in a reasonable time frame, we may undertake a review of the terms of your supplier contract with Bank of Ireland. This may include order reduction or, ultimately, in accordance with any applicable contractual right(s), termination of your supplier contract with Bank of Ireland.

FSQS will request evidence covering these topics, and you should provide as much information as possible where requested. We reserve the right to review your policies, procedures or any other documentation related to the requirements set out in this document. In some higher risk instances, we may undertake an on-site or desk based audit to validate your adherence to applicable Policies and the Code of Supplier Responsibility.

The provisions in this document are in addition to and not in lieu of any legal agreement or contract.

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 get in touch with any feedback or questions you have:

Contact your Bank of Ireland Relationship Manager