Supplier Policies

April 2024

FINAL V 1.1

Public

nationwide

Introduction

Nationwide's Supplier Policies set out what we expect from our suppliers to address the key areas of risk that Nationwide faces.

Compliance with our policies helps Nationwide to:

- Ensure operational resilience and prevent service disruption.
- Protect customers by ensuring the delivery of good customer outcomes.
- Operate in a green, inclusive and ethical manner, aligned to our Mutual Good Commitments.
- Meet our regulatory obligations, including Material Outsourcing and Non-Outsourcing.

These policies are shared with prospective suppliers during the tender process and align to our contractual agreements. We conduct regular control tests to check adherence to the requirements.

The policies are reviewed annually, or as the need arises to reflect internal or external changes. Key updates made since the previous version, are detailed on the final page.

The policy topics included in this document are:

- Business Continuity
- Communications
- Complaint Handling
- Conflict of Interest
- Data Governance
- Economic Crime
- Fraud
- Health & Safety
- Information Security
- Market Abuse Risk
- Payments
- Physical Security
- Pre-Engagement Vetting
- Product Lifecyle
- Technology
- Third Party Risk
- Vulnerability
- Whistleblowing

Our Supplier Policies supplement Nationwide's use of the Financial Services Qualification System (FSQS) online portal, for suppliers to submit relevant policy and control information related to their organisation. Further information about FSQS can be found on the "Working with Nationwide" page on Nationwide.co.uk.

Our Third Party Code of Practice, which sets out the environmental and social standards we expect our suppliers to uphold, sits separately to this document and can also be found via the link above on Nationwide.co.uk.

Requirements

Nationwide's suppliers are required to:

- Comply with our Third Party Code of Practice.
- Provide details on their organisation's policies and controls through completing the FSQS process and maintain their information in the system.
- Comply with the requirements set out in the document and be able to evidence adherence, where this is relevant to the service being provided to Nationwide.
- Inform Nationwide (Procurement Manager / Relationship Owner) if they're unable to comply with any of the requirements set out in this document where applicable.
- Take any necessary action to ensure they meet Nationwide's policy and control requirements.
- Share the requirements set out in this document with relevant personnel within their organisation and subcontractors that support the service to Nationwide.
- Inform Nationwide if there are any changes in compliance with the requirements set out in this document.

Please contact Nationwide for further clarification on the requirements set out in this document if required.

Business Continuity

Requirement	Description
Business Continuity Planning	Suppliers must have the following: • Industry Standard Approach to Business Impact Analysis. • Business Impact Analysis that is specific to Nationwide Services, completed within the last 12 months. • Business Continuity Plans and recovery strategies for all critical processes, which contain the scope, dependencies, roles and responsibilities, invocation and recovery procedure. • Business Continuity Plans appropriately approved by relevant individuals on a minimum annual basis and/or at point of material change. • Formally documented contingencies in the event of the Loss of a Critical Supplier, Loss of Critical System or Loss of Key Person. • Test multi-regional fail over capability on a minimum annual basis and/or at point of material change (material change being but not limited to changes in: process, systems, people, premises). • Documented Strategic Recovery Plans and Playbooks to cover the following loss pillars: Loss of People, Site, Systems and 3rd Parties. Including but not limited to Pandemic, Cyber, Severe Weather, Civil Unrest and Terrorism.
Training & Awareness	• Minimum mandatory training requirements for Business Continuity & Incident Management identified and documented. • A training programme for those with roles within Business Continuity & Incident Management. • Monitoring process in place to understand competence in role. • Business Continuity & Incident Management awareness across your organisation.
Site Loss	• Workload Transfer Arrangements and Remote Working Recovery Plans documented.
Exercising	• Documented Methodology and Approach in place for Exercising, and Exercise Site Loss strategies. • Exercising programme for organisational Plans, Playbooks and Incident Management Procedures and Business Continuity is in place, exercised on a minimum annual basis and/or at point of material change. • Post Exercise Reports produced for all exercises that include, Test Objective, Test Scenario, Participants, Success Criteria, Test Results and a List of recipients for the test report. • Identified corrective actions tracked to completion and escalated through respective governance.
Incident Management	• A proportionate standard methodology and approach to Incident Management, that includes Threat Analysis. • Incident Management Response includes a Communication Plan outlining how interested parties are notified and within what timeframe.

Business Continuity

Requirement	Description
Change Engagement	• An approach in place to ensure change do not cause disruption and is undertaken with Business Continuity considerations in mind. • Business Continuity & Incident Management Requirements are in place and operated to ensure that Change does not cause disruption to services. • Evidence of a proportionate Governance Framework that monitors the consumption of Cloud.
Supply Chain	• Due Diligence undertaken and Business Continuity provisions included in contracts with Suppliers, which you are dependent on delivering Services to Nationwide. • Gain assurances over critical supply chain BC/DR provisions.
Leadership	• Accountability for Business Continuity is formally assigned to Senior leaders and roles and responsibilities are documented and understood. • Documented and approved Business Continuity Policy is in place and implemented and reviewed on a minimum annual basis and/or at point of material change.

Communications

The following requirements are applicable to suppliers who create, review, approve, distribute, monitor and maintain communications that are sent to, or made available to for Nationwide customers.

Requirement	Description
Customer Understanding and Testing	Suppliers must have the following: • A robust process for identifying those communications, which are most likely to cause harm. These communications must be tested to assess the extent to which customers understand them, both pre and post distribution. *Further detail:* • *Suppliers must know:* – The specific communications they own (including those required by regulation) within their processes, – Which communications have the most risk of customer harm (i.e., they are not understandable, or not provided in a timely way) – When communications they own need to be distributed, and – The target audience for the communications (including the nature and scale of characteristics of vulnerability *that exist within the target audience).* • *Be clear on those communications which are likely to have the most risk of customer harm so they are identified and prioritised for consideration for customer understanding testing (pre-distribution).*
Communications Approval	• Processes in place (and operated in practice) to make sure that communications are approved by the right subject matter experts to ensure that they are accurate, understandable, and meet all legal and regulatory requirements. *Further detail:* • *Operate a Communication Approval Control to ensure communications support customer understanding, are accurate, clear, fair and not misleading. This approval control ensures, for those suppliers responsible for creating communications, that:* – *The Subject Matter Experts (SMEs) with the appropriate expertise and knowledge have reviewed and* approved the content. This will also ensure that approvals are captured by these SMEs within the relevant workflow / governance tool. – Information and data is accurate, on brand, meets legal / regulatory requirements and any claims can be substantiated (e.g., if we make claims something is 'green' or 'best', it can be validated with recent evidence). – Communications consider the needs and characteristics of the target audience, including vulnerable customers, to ensure we deliver good outcomes to all customers regardless of their communication needs.
Communications Change	• Robust processes in place and execute against these when changes to communications are identified. This includes: – Identifying that a communication needs to change, – Sharing the required change with all relevant stakeholders (both supplier and Nationwide) so that other relevant communications that are impacted can be assessed, and – Making changes to communications when they are made aware of any changes that are required. *Further Detail:* • *Where change is required to communications (for example due to updates to products or services), a Communication Change Control is operated. This is to ensure change is identified and acted upon so that existing communications are up-to-date and remain accurate*

Communications

Requirement	Description
Communication Distribution	• A list of mandatory communications (those required for legal or regulatory purposes) and understand when they should be distributed, when (if specific regulations stipulate), and the intended audience / volume. • Reconciliations must be carried out on communications which are mandatory and / or likely to cause harm to customers. • For example, customers are negatively impacted by a communication, i.e. a communication is not provided in a timely fashion or not provided at all, preventing them in achieving their financial objectives. • Where it is identified that communications are not sent as intended, then remedial action must be taken and this documented. *Further Detail:* • *Operate a Communication Distribution Control for those suppliers distributing communications. This is to ensure that communications can be reconciled to identify whether they are being provided to the intended target audience, and at the intended time, with remedial action taken where this isn't the case.*
Quality Checking	• For the parts of the communications process the suppler is responsible for, have robust processes in place to identify whether there are any critical points where a failure would result in a communication being inaccurate, not being understandable and / or not being distributed / provided in a timely way (or not being distributed / provided at all). • For these critical points, carry out sample-based Quality Checking (QC) to prevent and detect failings occurring, and to identify and correct any harm that has occurred. • Ensure a documented feedback and remedial action loop exists, so that any issues or errors are rectified within a reasonable period. Management information exchange should be agreed with Nationwide and provided as contracted. *Further Detail:* • *For those parts of the communication process the supplier responsible for, they must identify the critical failure points which could go wrong (i.e. cause harm). For example, those which would result in a communication not being provided when it should (or at all), not written in a way which is understandable, or customers don't take the action we expect.* • *For these critical points, the supplier must ensure that sample-based quality checking (QC) is carried out, at a volume and frequency that provides assurance the process is working as expected, and to prevent failings from happening. Where failings are identified, these should be corrected, and any harm redressed.*

Requirement	Description
Management Information and Monitoring	• Management information (both qualitative and quantitative) that is reported to and monitored by Nationwide. This should show adherence to the requirements set out in this policy. • Where suppliers are operating outside of tolerance or appetite, the reasons must be identified, specific timebound actions acted upon and evidence recorded for any remedial action taken. • Provide the relevant management information as per contractual obligations and on ad-hoc request. *Further Detail:* • *Share with Nationwide, Management Information that demonstrates the extent to which communications are:* – *Understood by our customers.* – *Driving the intended customer action.* – *Accessible, accurate, clear, fair and not misleading.* – *Issued to the target audience in a timely way in a format that is appropriate to their needs.* • *Where actual or potential issues are identified, action must be taken to address this, and evidence retained.* • *Testing must be conducted on a sample of communications, post-distribution to understand whether good outcomes are being achieved for our customers when they are communicated with.* • *The volume and frequency of testing must be adequate to identify whether customers understand a range of communications.*

Key Terms	
Communications	In scope communications are those that are published, broadcast, or sent to more than one customer, or templates for tailored communications which can be sent to more than one customer. Those communication sent to only one customer are subject to the controls and requirements set out on the Product Lifecycle page (p.X) in this document. Communications are the means of providing information to our customers from NBS, its subsidiaries and suppliers. Communications can be verbal, visual or in writing and include: physical communications (e.g., letters, marketing material), digital content (e.g., website, internet bank, email, texts) and scripts for verbal interactions with customers
Communication Process	The end-to-end process of identifying the communication needs for creating, approving, reviewing, changing, and distributing communications.
Consumer Duty	Financial Conduct Authority (FCA) regulations set higher and clearer standards of consumer protection across financial services and requires firms to put their customers' needs first. The collection of rules and guidance are collectively known as the Consumer Duty.

Key Terms

Communications Creator	A firm which designs and writes (creates) communications. This could be Nationwide or a supplier.
Communications Distributor	A firm which distributes communications to (shares information with) Nationwide customers. This could be Nationwide or a supplier.
Harms	Harms can occur where customers are negatively impacted by a communication, i.e. a communication does not enable a customer to achieve their financial objectives. This could be caused by a communication not reaching them, or being misleading / misunderstood, or not clear enough that action is required. For example, customers given incorrect / misleading information; information not provided in a timely fashion.
Vulnerable Customers/ Vulnerability	Someone who, due to their personal circumstances, is especially susceptible to harm, particularly when we are is not acting with appropriate levels of care. Vulnerability can include one or more characteristics such as health, a life event, financial resilience, or financial capability.

Complaint Handling

The following requirements are applicable to suppliers providing services that involve contact with customers (theirs or Nationwide's), either face to face, via telephone, internet, email, social media or written letter.

Requirement	Description
Internal Complaints Procedure	Suppliers must have the following: • A Complaints Policy / Framework that includes: – A complaints definition that aligns to the FCA's definition of a complaint. – A documented process for managing complaints received from the Financial Ombudsmen Service (FOS), which includes sharing outcomes and learnings from complaints. – How vulnerable customers are supported. – A system that facilitates the management of complaints. – Defined mandates for staff to offer compensation / redress. – Regular guidance / training given to all customer facing personnel – Complaints performance MI reported to Senior Management. – An annual review of the Policy/Framework, involving 2nd (Compliance) and 3rd (Audit) line oversight.
Complaints Quality Assurance	• A Complaints Quality Assurance (QA) Model that includes: – Documented frequency and volume/percentage of complaints checked. – Assessment of Good Customer Outcomes for each case. – Assessment of adherence to regulatory requirements related to complaints. – A review of the initial complaint call or correspondence to ensure all points have been correctly identified /addressed. – A risk based approach taken to complaints QA, (e.g. an increased level of checking on new starters or to support where under-performance is identified). – Independent QA checking undertaken by a separate function to the complaint handling team. – A check-the-checker model to review consistency/accuracy of checking completed by the QA function. – Sharing QA feedback with team/handlers. – A process to ensure remedial action is undertaken where a poor/incorrect outcome has been identified. – QA output/MI reported to Senior Management.
Complaints Root Cause Analysis	• A Complaints Root Cause Analysis (RCA) Model that includes: – All complaints, including those resolved within the FCA's 3 Business Day timeframe – RCA outputs / MI reported to Senior Management
Complaints Training & Competency	• A Complaints Training and Competency Framework that: – Applies to all customer facing staff. – Includes a defined process for how dedicated complaint handlers attain competency. – Covers soft skills (e.g. call handling and how to approach conversations with customers), for handling complaints and regulatory requirements. – Is reviewed annually.

Conflicts of Interest

Requirement	Description
Employee Training	Suppliers must have the following: • Training for employees to ensure they understand how to recognise conflicts of interest, and their associated responsibilities.
Processes & Controls	• Effective processes and controls to ensure that conflicts of interest are identified, disclosed, managed and recorded.
Record Keeping	• Record conflicts of interest in a register and share it with a Nationwide Senior Relationship Owner (SRO). • The register must include details of each potential or actual conflict of interest; and the associated controls/actions taken to prevent or mitigate the conflict.
Engagement with Senior Relationship Owner	• Discuss identified conflicts of interest that may impact Nationwide and/or our customers with the SRO, specifically the controls/actions taken to prevent or mitigate any impact to Nationwide and/or customers.
Review Conflicts of Interest	• Review recorded conflicts of interest on a regular basis (e.g. minimum annually).
Policy Breaches	• Report any breaches of this policy to the Nationwide SRO.

Key Terms	
Personal Conflicts of Interest	A situation which could cause an employee to put their own interests (whether professional or personal) or those of a close personal relationship or a close family member's interests before the interests of a customer or Nationwide. This includes situations which could potentially affect an employee's work, independence or decision making.
Organisational Conflicts of Interest	A situation where Nationwide's arrangements, activities or its structure could put either Nationwide's or its employees' interests above those of our customers or create a conflict of interest between two or more of Nationwide's customers, where each is owed a duty of care. This includes situations arising from suppliers operating on behalf of Nationwide.

Data Governance

The following requirements are applicable to suppliers who will have access to Nationwide's data or are receiving and/or sharing data with us, (this includes holding, transporting, disposal, receiving, transacting or viewing of data).

Requirement	Description
Data Quality	Suppliers must have the following: • A Data Quality/Assurance policy to measure and report on the Data Quality Dimensions (completeness and conformity as a minimum) to ensure data is safe, secure, reconciled and managed in line with in-force standards/contractual clauses • The ability to identify Data Quality issues and undertake remediation/reconciliation as appropriate
Data Retention & Deletion	• A Data Retention/Deletion policy to review, retain and delete data in line with applicable law/legislation • A data deletion capability • A mechanism to identify and risk-assess non-compliance with law/legislation/Nationwide's Retention Schedule/contractual clauses and to create and deliver on a remediation plan

Please also see the Information Security requirements set out on page 13-14.

Requirement	Description
Roles & Responsibilities	Suppliers must have the following: • Defined responsibilities and accountabilities for employees, Senior Managers and the escalation routes available under governance.
Risk Assessments	• Business wide risk assessments that establish overall economic crime risks and assess the effectiveness of the systems and controls applied to mitigate them.
Due Diligence	• Initial and ongoing due diligence, risk assessment and screening applied to business relationships, including employees, customers, suppliers and associated parties. • Enhanced due diligence controls where a relationship is deemed of a higher risk such as, but not limited to, higher risk countries or Politically Exposed Persons (PEPs).
Process	• Processes (including transactional monitoring) to internally detect, investigate and report suspicious activity. • Processes to ensure that mandatory fund transfer information is included in electronic payment messages.
Screening	• Screening of payments and parties to identify and escalate potential matches to relevant sanctions regimes.
Record Keeping	• Record keeping, management information and governance (including escalation) requirements.
Training	• Training requirements (including specialised training for certain business areas), in relation to money laundering, countering terrorist financing, bribery and corruption (including tax evasion), financial sanctions, fraud (internal and external), market abuse and insider dealing, conduct risk and whistleblowing
Control Testing	• Independent testing (Compliance / Internal Audit Function) of the economic crime controls, to ensure appropriate assurance of an effective compliance programme.

Requirement	Description
Roles & Responsibilities	Suppliers must have the following: • Roles and responsibilities clearly assigned, processes fully documented, appropriate training provided and all activities subject to appropriate monitoring. • Roles and responsibilities reviewed regularly (and in any event not less than once every 12 months) and after any material change to the supplier operating model or business.
Fraud Suspicion Reporting / Whistleblowing	• A suspicion reporting mechanism/process in place to ensure any fraud concerns are reported, assessed and investigated as appropriate by an internal centralised team. • All confirmed fraudulent cases reported to NBS (where they relate to NBS services) and the relevant authorities and industry bodies. • Operate an appropriate confidential internal process for raising concerns which may relate to fraud, and make colleagues aware of any other whistleblowing routes externally.
Fraud Education & Awareness	• Employee fraud education and awareness training delivered annually for all employees, contractors, and third-parties • All individuals with access to Nationwide or Nationwide member data/ information receive appropriate education and awareness training, to ensure there is clear understanding of how this information should and should not be used. • The levels of fraud education, training, and awareness adequately cover the fraud risks and controls different roles may be exposed to, and recorded with a robust audit trail of evidence.
Authentication	• Where the supplier is dealing with Nationwide customers or employees, a robust authentication process to support any processing or handling of member requests, information or transactions. • Where applicable, this adheres to the requirements of 'Strong Customer Authentication' in line with the Regulatory Technical Standards, which form part of the Payments Services Directive 2.
Fraud Loss Events	• A fraud loss event (incident) management and reporting process that identifies, assesses, escalates, and ensures an appropriate response to fraud incidents or loss events. This will also include suppliers that provide a platform for Nationwide's fraud detection systems. • Tailored written incident response plans for each category of known fraud risk/incident that defines the roles of personnel, escalation mechanisms, and phases of incident handling/management.
Fraud Policy	• A fraud policy that is reviewed annually and made available to all employees, contractors, and Third Parties.
Production of Tokens	• If applicable, a robust process when producing or handling tokens for Nationwide (including cards, chequebooks and PIN's) to ensure there is adequate and appropriate segregation of duties or dual control, physical security, secure destruction procedures, full audit trails of actions and robust management oversight.

Requirement	Description
Service Provision	Supplier's personnel must: • Perform, manage and provide the services in a safe manner and free from any unreasonable or avoidable risk to any person's health or safety.
Rules & Regulations	• Whilst on Nationwide's premises, comply with all rules and regulations (such as, by way of example only, health, safety and fire procedures).
Supervision & Training	• Be properly supervised and sufficiently trained, and informed about all relevant rules, procedures and statutory and regulatory requirements concerning health and safety and safety at work

Fire Safety

- Nationwide aim to comply with the requirements of relevant Fire Safety Regulations and all other current applicable fire safety standards.
- We commit to providing a working environment that supports the fire safety of employees, customers and suppliers. Nationwide, with the help and support of the NGSU, work to develop and promote effective policies and practices. You have an active role in managing fire safety.
- The overall responsibility for fire safety precautions sits with the Chief Executive and Directors and are exercised through the Chief Safety Officer and other competent persons.
- As a business we recognise that incidents can occur and it's our responsibility to ensure that there are appropriate management controls in place to investigate.
- Fire legislation requires everyone including the management team and third-party contractors to work together to reduce or eliminate fire risks at work.
- The identification, assessment and control of fire risks are a managerial responsibility of equal importance to all others. Also, you must take all reasonable steps to ensure your own personal health and safety, that of your colleagues, our customers and third-party contractors.
- By working in partnership with West Midlands Fire Service there is an agreed approach to fire safety management ensuring that appropriate policies, procedures and governance structures are in place to meet legislative and best practice requirements. We'll consult with the NGSU in the making and maintenance of effective arrangements for fire safety. We'll provide such resources, financial and otherwise, necessary to meet our responsibilities.

Information Security

The following requirements are applicable to suppliers who will have access to NBS data, IT infrastructure/systems or unaccompanied access to restricted locations. (This includes the holding, transporting, disposal, receiving, transacting or viewing of data). More specific security requirements for each service will be assessed and agreed on a case-by-case basis.

Requirement	Description
Identify	Suppliers must have the following: • Asset Management - all systems, devices, applications, data, personnel and partners catalogued in a centralised register and managed, consistent with their relative importance to the objectives and risk appetite. • Governance - regulatory, legal and operational requirements understood and inform information security policies, procedures and processes. • Risk Assessment - the information security risks to assets and operations identified and reported. • Risk Management Strategy – information security risk tolerance clearly defined and communicated. • Supply Chain Risk Management - information security risks associated with suppliers and partners identified and managed in accordance with risk management processes.
Protect	• Identity Management and Access Control - access to systems, devices, applications and data is limited to authorised users and processes. • Awareness and Training – personnel and partners provided with role-appropriate information security awareness education and must be trained to perform their information security-related duties and responsibilities, consistent with related policies, standards, and agreements. • Data Security - information security controls implemented to protect the confidentiality, integrity, and availability of data. • Information Protection Processes and Procedures - information security policies, processes, and procedures documented and maintained to ensure the protection of systems, devices, applications and data. • Maintenance & Repair - maintenance and repairs to systems, devices and applications performed consistent with information security policies and requirements. • Protective Technology - security controls implemented to ensure the security and resilience of systems, devices, applications and data, consistent with the information security policies, standards and agreements.
Detect	• Anomalies and Events - anomalous activity on systems, devices and applications detected and the potential impact of events assessed. • Security Continuous Monitoring - systems, devices, applications, data, personnel and partners monitored to identify information security events and to verify the effectiveness of current controls. • Detection Processes - detection processes and procedures continuously evaluated to ensure they are well defined and meet requirements.

Requirement	Description
Respond	• Response Planning - recovery processes and procedures executed and maintained, to ensure restoration of systems or Information Systems affected by information security incidents. • Communications - response activities coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies) • Analysis - analysis conducted to ensure effective response and support recovery activities. • Mitigation - response activities performed to prevent expansion of an event, mitigate its effects and resolve the incident. • Improvements - response activities improved by incorporating lessons learned from current and previous detection/response activities.
Recover	• Recovery Planning - recovery processes and procedures executed and maintained, to ensure restoration of systems or Information Systems affected by information security incidents • Improvements - recovery planning and processes improved by incorporating lessons learned into future activities. • Communications - restoration activities coordinated with internal and external communication experts.

Market Abuse

The following requirements are applicable to suppliers should they be in possession of inside information relating to Nationwide, to prevent/detect potential market abuse. A breach of these guidelines may be a criminal or civil offence or regulatory breach.

Requirement	Description
Training	Suppliers must have the following: • Employees fully understand their roles and responsibilities for complying with UK Market Abuse Regulation. Supported through training and guidance with regular performance reviews completed by managers. • Adequate and up to date guidance, policies and procedures in place to identify, control and detect / prevent market abuse from occurring. • Agreed and documented roles and responsibilities for managing inside information relating to Nationwide.
Identification and Control of Inside Information	• Able to evidence effective controls in place to identify any inside information relating to Nationwide and this information is strictly controlled (such as restricting access to electronic folders); only shared with Nationwide's permission; and the firm must be able to evidence that it has adequate procedures for identifying and reporting the misuse (accidental or deliberate) of such information. • Segregation of systems and duties where appropriate to limit or reduce the chance of market abuse occurring, such as (but not limited to) logical / physical segregation as well as ongoing monitoring of such systems.
Insiders list	• Nationwide is made aware of all persons who are in receipt of Nationwide inside information and that the required personal details are provided to Nationwide for inclusion on the Insider List. • Nationwide is made aware of any changes in circumstance or details, of any persons included on the Insider List
Communication and Disclosure	• Public announcements that could contain inside information relating to Nationwide are not shared without consulting Nationwide. • The content and timing of such announcements are made with the consent of appropriate senior representatives of the firm and published through an approved Primary Information Provider. • Contingency plans defined for handling cases where inside information is leaked, or knowingly false information is disseminated to the public, before the planned announcement date.

Market Abuse

Key Terms	
Inside Information	Information of a precise nature which has not been made public, relating directly or indirectly, to one or more issuers or to one or more financial instruments; and which if it were made public, would be likely to have a significant effect on the prices of those financial instruments or on the price of related derivative financial instruments.
Insider Dealing	Where a person possesses inside information and uses that information by acquiring or disposing of, for its own account or for the account of a supplier, directly or indirectly, financial instruments to which that information relates.
Unlawful Disclosure	Where a person possesses inside information and discloses that information to any other person, except where the disclosure is made in the normal exercise of an employment, a profession or duties.
Market Manipulation	Entering into a transaction, placing an order to trade or any other behaviour which gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a financial instrument, or secures, or is likely to secure, the price of one or several financial instruments.
Disseminating Information Likely to give a False or Misleading Impression	The act of spreading, or causing the spread of, information which gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a financial instrument, including the dissemination of rumours, where the person who made the dissemination knew, or ought to have known, that the information was false or misleading.

Payments

The following requirements are applicable to suppliers that are involved in payment transaction processing for Nationwide including:

- Providing the IT infrastructure to process payment transactions
- Processing payment transactions on behalf of Nationwide (payment transactions into Nationwide customer's accounts/payment transactions out of Nationwide customer's accounts).

Requirement	Description
Transaction Data Accuracy	Suppliers must have the following: • Independent checks on a percentage of payment transactions (recommend 5%-10%) to assess completeness and accuracy, carried out by a fully competent member of staff, prior to the completion of the transaction (for outbound payments), or application to an account (for inbound payments). • A risk based approach to determining the percentage of transactions subject to Data Accuracy Checks. This risk based approach is documented, along with the payment transaction attributes subject to checking and approved by management. • All errors identified following Transaction Data Accuracy checking corrected (retrospectively if checking occurred after completion) and these payment transactions are subject to re-checking, to ensure accuracy. • Reports, documenting the results of Transaction Data Accuracy Checks, produced and made available to management to address performance and/or ensure appropriate remediation is taken to prevent recurrence.
Documented Processes	• Documented processes to provide employees with relevant step-by-step reference material. • Process documentation must be: – Reviewed annually or earlier if changes to the document are required, such as the process or any associated regulations or scheme requirement has changed for example. – Approved by an appropriate person such as a manager of appropriate level or delegate, be version controlled and easily accessible to all staff involved in the process. – Formally communicated to relevant staff following any updates and confirming where the documents can be accessed.
Payment Transaction Data Integrity	• Integrity and accuracy of payment transaction data maintained throughout the payment cycle (from initiation to settlement of the payment), by ensuring that the payment information: – Is processed and settled in line with the original request, applicable regulations, law, and scheme requirements; and – Cannot be modified without detection – Remains original throughout its life cycle. • In exceptional circumstances, where transactions may need to be amended due to an error by the initiator, a tamper proof audit trail including authority from the initiator of the payment instruction, is maintained to evidence that the change was required to process the transaction and that the initiator of the payment instruction has agreed to the changes.

Requirement	Description
Formal Approval of Payment Transaction SLAs	• Service Level Agreements (SLAs) for payment transactions (outgoing payments, incoming payments, internal transfers) agreed with the appropriate Nationwide representative, (such as the Nationwide Senior Relationship Owner, Relationship Owner, or Operational Owner) to ensure payment transactions meet the required Payment Services Regulations (PSR).
Payment Transaction Timeliness	• Payment transactions (outgoing payments, incoming payments, internal transfers) executed in a timely manner, meeting relevant Payment Service Regulations (PSR), as formally agreed with NBS (SLAs agreed).
Payment Transactions Management Information (Timeliness)	• Payment transaction SLA monitoring (outgoing payments, incoming payments, internal transfers), to ensure relevant Payment Services Regulations (PSR) and the SLAs agreed with NBS are met. • Monitoring reported against approved SLAs and where outside of these approved SLAs, specific, timebound and governed action plans are in place to resolve this, and reported to the appropriate Nationwide representative (such as the Senior Relationship Owner, Relationship Owner, Operational Owner), to provide oversight of the PSR compliance position and maintain ongoing adherence.
Regulatory, Legal, Scheme Requirements Adherence	• Suppliers involved in the processing of payment transactions (outgoing payments, incoming payments, internal transfers), ensure that all relevant Payment regulations, law, scheme requirements, and/or Industry Standards, within their processing, are identified, understood and controls are in place to achieve and maintain compliance. • Suppliers engage with NBS Subject Matter Experts (SMEs) to understand the requirements applicable to their processes.
Regulatory, Legal, Scheme Requirements Adherence (Change)	• During the design stage of any change impacting the processing of payment transactions (outgoing payments, incoming payments, internal transfers), a mapping exercise is conducted by the 'Change Programme/Project' to identify relevant Payment regulation, law, scheme requirements, and/or industry standards. • The mapping exercise is documented and maintained by the Change Programme, evidencing stakeholders engaged, the requirements considered, and the approved decisions made. • Following the identification of relevant regulatory, law, scheme requirements and/or industry standards, the design and build phase ensures appropriate controls are implemented to meet requirements, mitigating risk of non-compliance, and maintaining ongoing compliance once in BAU.
Payments Transaction Processing Training & Competency	• Individuals involved in the processing or authorising of a payment transaction (outgoing payments, incoming payments, internal transfers) complete sufficient training to be deemed competent for their role, including knowledge of any relevant payment regulatory, legal or scheme requirements impacting the process they operate. • Ongoing competence assessed, monitored, and maintained (e.g. through competency testing, Transaction Data Accuracy Checks (QA/QC), e-learning, refresher training, MI). • Documented process/approach to evidence how staff are appropriately trained and competency is maintained.

Physical Security

The following requirements are applicable to suppliers providing services that originate, receive, store, process, destroy or forward Nationwide information.

Requirement	Description
Physical Security - Policy	Suppliers must have the following: • A formally documented physical security policy with underpinning standards, processes and procedures with a nominated individual or role accountable for physical security.
Physical Security Risk Assessment	• A Physical Security Risk Assessment undertaken on a regular basis for all facilities where services are provided to originate, receive, store, process, destroy or forward Nationwide physical assets to identify credible physical security threats that may impact business operations at the premise. • A risk rating applied to the facility and a Vulnerability Assessment undertaken to inform required physical security control measures. • As a minimum, the risk and vulnerability assessments reviewed on a cyclical basis at pre-defined intervals (minimum annually), or in response to received threat intelligence or as part of a Post Incident Review.
Secure by Design	• Utilise a secure by design project lifecycle during the development of a New Facility or transformation of an In-Use Facility, including specifying physical security requirements and validation that physical security requirements are met prior to go live. • A risk profile generated by the physical security risk assessment process for the facility, to determine the required technical build configuration baseline standards (aligned with industry benchmarks). • Where non-conformances to the Build Standard are required, these are raised and logged as a Dispensation or Waiver and notified to Nationwide.
Secure Build Physical Security Control Measures	• In-place physical security control measures (barriers, lighting, glazing, doors etc) implemented at facilities or work areas, where services are provided to originate, receive, store, process, destroy or forward Nationwide Information. • In-place physical security control measures provide a known level of security performance and align with recognised industry benchmarks such as the Loss Prevention Certification Board (LPCB) or CPNI Catalogue of Security Equipment (CSE).
User Authentication and Access Control	• Access through the secure perimeter into non-public areas of facilities, or work areas where services are provided to originate, receive, store, process, destroy or forward Nationwide Information or sensitive operational areas (such as server or plant rooms), are restricted to authorised individuals who are authenticated prior to access being granted. • Once authenticated, entry is permitted using an appropriate access control mechanism (e.g. Automated Access Control System and tokens, manual / mechanical keys or receptionist), which are capable of maintaining an auditable record of all entry and exit to the building or area. • Records of entry & egress retained for a period no less than 90 days. • Access permissions linked to the Joiners, Movers & Leavers process and promptly revoked when no longer needed

Physical Security

Requirement	Description
Visitor Management	• All visitors to non-public areas of facilities or work areas where services are provided to originate, receive, store, process, destroy or forward Nationwide Information are registered and issued with a security pass, which makes them easily identifiable as a visitor. • The visitor is escorted by an employee of the supplier when in the non-public space of the building / area and returns any security passes on exit from the premises. • The register of visitors is auditable and retained for a period not less than 90 days.
Incident Management	• Physical Security incidents identified, reported and responded to, in accordance with documented incident management procedures. • Root cause analysis performed to identify recurring issues that require risk management response, or where risk appetite has been exceeded. • Nationwide notified when a physical security incident which has, or had potential to impact Confidentiality, Integrity or Availability of Nationwide physical assets.
Security Education and Awareness	• Employees and contingent workers provided with relevant and targeted security education, training and awareness based on an assessment of training needs on at least an annual basis.
Physical Security Event Monitoring and Incident Response	• Facilities that are not 24/7 operational incorporate an Intruder Detection System (IDS), with detection sensors on all outer perimeter points of entry (doors and windows) to buildings or work areas, where services are provided to originate, receive, store, process, destroy or forward Nationwide Information. • The IDS terminates at a Security Control Room where operators are able to verify alarms and deploy and a response force to contain and respond to the event, (either via in house security officer, visiting key-holder or Police response). • Where installed, all electronic security systems (CCTV, Intruder Detections Systems, Automated Access Control Systems) are installed and maintained by an approved certified supplier (either SSAIB or NSI).

Pre-Engagement Vetting

The following requirements are applicable to suppliers where their employees have unchaperoned access to Nationwide premises, data or systems.

Requirement	Description
Identity Check	Supplier's pre-employment vetting must include the following checks: • Identity verification – using valid, original photographic evidence and a copy retained as evidence. – *To prove that the individual is who they say they are.*
Address Verification	• Current address and address history is cross-referenced with databases including the electoral roll. – *To confirm where the individual lives.*
Criminal Record Check	• Details of criminal convictions considered unspent, under The Rehabilitation of Offenders Act 1974. • The individual's name against the relevant UK jurisdictional agency – the organisation that holds details of legal decisions and judgements. • Where applicable, an overseas criminal background check to see whether the individuals name exists on any criminality databases in other countries. – *To check that the individual is of good character and helps guard against inappropriate disclosure of information by individuals with criminal or malicious intent.*
5-year credit check	• A credit and bankruptcy check of the individual, via law enforcement or other legal agencies and a copy of the credit report retained on file. – *To reveal any individual who may pose a conflict of interest risk if the candidate is under financial pressure outside of the work environment.*
Right to Work	• Obtain the original appropriate government-issued documentation to confirm the individual is legally entitled to work in the UK and a copy is retained as evidence. – *To verify that the individual is legally entitled to work in the relevant jurisdiction(s).*
2-Year Academic Qualifications/ (where required for the role)	• Verification that any academic/professional qualifications declared are valid and held to the level stated. – *To confirm that the individual has the suitable qualifications for their role.*
2-Year Occupational History and Written References (CV check)	• Employment and education history for the last two years. – *To check the suitability and integrity of the person; that career gaps greater than three months are investigated and assessed to ensure that all information on previous employment is accurate; and that previous employers are genuine.*
Sanctions Check	• Check against any official sanctions lists or restricted activity matrices, to prove compliance with applicable sanctions laws. – *To check if an individual is on a government and other sanctions list, which may pose regulatory or reputational risk for Nationwide.*

Pre-Engagement Vetting

Requirement	Description
CIFAS	• Where the supplier is providing workers to Nationwide, (providing goods or services which do not involve the provision of workers to Nationwide is out of scope) - a search conducted in the Credit Industry Fraud Avoidance System (CIFAS). • The search is conducted against both the Internal Fraud Database and the National Fraud Database. – *To confirm that the individual is of good character, and helps guard against inappropriate disclosure of information by individuals with fraudulent history*
Politically Exposed Person Check	• Identify whether the individual - has Politically Exposed Person (PEP) status, is an immediate family member of a PEP, or is a close associate of a PEP (e.g. in a close business relationship with a PEP). • In the event an individual meets any of the above criteria, inform Nationwide and agree a solution as appropriate. – To guard against the risk of PEP status being used to exert improper influence for or on behalf of Nationwide.
Media Search	• A search using full name against open source internet data sources for any adverse media coverage. • Date of birth and address is used to narrow down the search to ensure validity. – To check for individuals who may pose reputational risk.
Incomplete Checks or Adverse Results	• Supplier follows the contractual process for dealing with incomplete checks or adverse screening results. This may involve further discussion with the individual, completion of a declaration of fact, or a risk assessment to determine if engagement can still take place – To verify that Supplier personnel are not automatically assigned to Nationwide if the required evidence for a check cannot be gathered for an individual, or if they fail a check
Regulated Screening	• For roles requiring regulatory approval/certification - full screening confirmed and completed by Nationwide at the time of on-boarding – To confirm that an individual has the required approval from the regulator and that they are deemed 'fit and proper' to prevent regulatory risk.

Product Lifecycle

The following requirements are applicable to suppliers carrying out product design (manufacturing), sales (distributing) and servicing activities for retail customers on behalf of Nationwide.

Supplier manufactures/co-manufactures a product and Nationwide distributes

Requirement	Description
Product Approval / Review Processes (including the sharing of value assessment and target market information)	Where suppliers design and manufacture products/services on behalf of, or act as subsidiary for NBS, the supplier must have the following: • A product approval / review process to adequately assess the product and distribution strategy, that enables the provision of the following information: – Relevant target market mapping – Fair Value assessments – Potential risks/harms to customers (including those in vulnerable circumstances) – Product testing information • Where Nationwide and a supplier are co manufacturers, roles and responsibilities are documented as part of the onboarding / review process.
Sharing of Management Information	• Management Information (both Qualitative/Quantitative) available, used and shared via agreed channels. – This is to understand whether customers (including those in vulnerable circumstances) are receiving good outcomes, regulatory requirements are being met, servicing is carried out within SLA's and whether harms are materialising. When outside of appetite, the reasons are identified and acted upon, with timebound actions in place. • Provide the relevant MI against agreed SLA's and on ad-hoc request.
Product and Service Review Process	• Products / services, sales journeys, and service / support journeys have a regular, or as required by regulation, point in time review to identify and rectify where they do not continue to meet the needs of the target market, offer fair value, avoid harms, provide good outcomes, and the right level of member understanding and support. • Provide the relevant MI against agreed SLA's and on ad-hoc request.

Supplier distributes / services customers on Nationwide's behalf

Requirement	Description
Quality Checking	Where suppliers are distributing / servicing on behalf of Nationwide, the supplier must have the following: • The critical points in processes that would result in member harm or poor outcomes identified and quality checked. There's a representative sample checked, with the frequency and who is carrying out the quality checks documented. • Provide the relevant MI against agreed SLA's and on ad-hoc request.
Sharing of Management Information	• Management Information (both Qualitative/Quantitative) available, used and shared via agreed channels. – This is to understand whether customers (including those in vulnerable circumstances) are receiving good outcomes, regulatory requirements are being met, servicing is carried out within SLA's and whether harms are materialising. When outside of appetite, the reasons are identified and acted upon, with timebound actions in place. • Provide the relevant MI against agreed SLA's and on ad-hoc request.

Supplier distributes / services customers on Nationwide's behalf

Requirement	Description
Training & Competency	• Where required by regulation, training and competency schemes are in place, to ensure employees are competent to carry out distribution or servicing activity, including identifying and managing customers in vulnerable circumstances.

Key Terms

Product Lifecycle	Product Lifecycle is the journey which every product and service goes through from initial research, ongoing management, through to withdrawal / closure
Consumer Duty	Financial Conduct Authority (FCA) regulations set higher and clearer standards of consumer protection across financial services and requires firms to put their customers' needs first. The collection of rules and guidance are collectively known as the Consumer Duty.
Manufacturer	The firm which creates, designs, develops, issues, operates, manages or underwrites a product or service including existing and closed book products. This could be Nationwide or a supplier.
Co-Manufacturer	A firm would be considered a co-manufacturer where they can determine or materially influence the manufacture or price and value of a product or service. This would include a firm that can determine the essential features and main elements of a product or service, including its target market.
Distributor	The firm which offers, sells, advises on, or provides customers with a product or service, or makes arrangements with customers with a view to entering an agreement for a specified investment. This could be Nationwide or a supplier.
Customers	'Customers' in this policy means all Nationwide Building Society product holders and future customers, whatever their customer rights. In this policy, reference to customers means all customers, including those in vulnerable circumstances.
Customer Service and Support	Done by a person or system, we support customers to navigate a journey, complete a task, or reach a specific outcome-helping them manage their products and services. This includes complaints, remediation, and supporting them through financial difficulties
Monitoring	Means the systematic and ongoing review and check of products / services, sales and servicing processes / strategies and communications. This is achieved through a combination of MI and point in time assessments and is to check whether good outcomes are being delivered, potential harms are being identified and mitigated, and regulations complied with.
Products and Services	When used together, the meaning 'products and services' describes the things that customers buy or sign up for to meet their financial goals.
Vulnerable Customer	Someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care. This may be because of their current circumstances that may give rise to different or additional needs. The risk of detriment arises not just from the customer's own circumstances but also from the interaction they are having with Nationwide and its suppliers. This includes change we may deliver that impacts an existing product or service.

Technology

The following requirements are applicable to suppliers providing services that include the use of technology.

Requirement	Description
Managing Solution Development Lifecycles **COBIT Ref: BAI03**	Suppliers must: • Be able to provide evidence of a solution development process/methodology.
Managing Technical Resilience **COBIT Ref: DSS04**	• Ensure that all technology systems/services required to support the delivery of Nationwide business and internal service lines are resilient across data centres and far apart enough to reduce the risk of data centres being impacted simultaneously by a single event. Nationwide would expect this to be a minimum geographical distance of 10 miles. • Identify scenarios and conditions which will affect the availability of the solution being supplied and have plans to mitigate these conditions. • Have recovery plan(s) for each technology system/service required to support the delivery of Nationwide business and internal service lines, with corresponding Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) in line with agreement with Nationwide. Ensure plan(s) are reviewed for accuracy at least once every 12 months. • Test and validate recovery plan(s) which demonstrate that technology systems/services and data can be recovered to meet the requirements stipulated by Nationwide. • Ensure that if any testing fails to achieve the minimum recovery requirements for the applicable resilience category, Nationwide are promptly notified and provided detailed remediation plans (including actions to be undertaken and corresponding completion dates). • Ensure ESCROW agreements are in place where appropriate to ensure continuity and provision of services.
Managing Agreements **COBIT Ref: APO09**	• Ensure that formal agreements with 4th Parties (e.g. cloud providers), which form part of solution(s) provided to Nationwide, are in place.
Managing and Maintaining Solution Backups **COBIT Ref: DSS04**	• Ensure that all technology systems and services used in the provision of services to Nationwide have adequate backup and restoration processes in place which operate in line with Nationwide requirements. • Ensure that all backup media associated with the provision of services to Nationwide, together with the arrangements for the handling of storage of those media, remain secure and reliable. • Ensure backup restoration is tested regularly, assuring that Confidentiality, Integrity and Availability of solutions and data is maintained - and provide regular attestation that restoration of data can be achieved within agreed SLA's, RTO's and RPO's.

Requirement	Description
Managing and Maintaining Technology Assets and Entities **COBIT Ref: BAI09**	• Identify all technology assets supporting the service provided to Nationwide and determine their criticality to the provision of service. • Record all technology assets accurately - and report "lost or stolen" assets promptly. • Procure and deliver technology assets through recognised and/or approved suppliers. • Manage and maintain all technology assets from procurement to disposal by managing the asset lifecycle effectively, efficiently and securely. • Ensure patch management solutions and schedules are in place which support the environments/services provided to Nationwide. • Ensure processes are in place to prioritise, manage and apply emergency patches, including backout processes where appropriate. • Ensure that all technology assets which store, process or control Nationwide information (including but not limited to data storage media and back up devices) are safely and securely deleted and disposed of at the end of their lifecycle/agreed usage with the society. Where assets are to be reused in the future, appropriate sanitisation standards must be followed. • Ensure licence management for hardware and software (including applications, plug ins and supporting tools) is in place and maintained. Ensure that licencing numbers are appropriate and accurate.
Managing Capacity **COBIT Ref: BAI04**	• Ensure that levels of performance and capacity for all key technology components used in the provision of service for Nationwide are defined in line with stated business needs. • Ensure that appropriate alerts and thresholds are defined and in place on key components to warn of potential breaching of thresholds. This must allow for appropriate remediation lead time and that these are reviewed periodically to ensure service delivery is aligned to Nationwide needs.
Managing Technical Change **COBIT Ref: BAI06**	• Ensure that all technology that is used in the provision of services to Nationwide is managed under a documented and governed change control process. • Ensure that all technical change that may impact the service provision to Nationwide is coordinated with Nationwide and approved. • Ensure that no change is made without appropriate authorisation and approval taking place prior to implementation. • Ensure that segregation of duties between the change initiator, owner, approver and implementer is in place. • Ensure changes are planned, managed and executed according to the level of associated risk. • Ensure changes take account of potential impact on performance and/or capacity of affected technology components. • Ensure changes undergo technical and business testing relevant to the change prior to implementation, with evidence retained. • Ensure changes are tested and monitored post implementation to ensure that they have been delivered successfully with no unplanned impact. • Ensure changes include backout and regression plans, in case of failure or negative impact. • Ensure an emergency change process is in place, including definition of what constitutes an emergency change - and details of when this process may be invoked.

Requirement	Description
Managing Technical Configuration **COBIT Ref: BAI10**	• Maintain a complete and accurate register for all in-scope configuration items used in the provision of services to Nationwide (including ownership and upstream/downstream dependencies/mappings). • Have internal controls in place that assure the ongoing maintenance of the accuracy, security and completeness of data, where data is owned/managed by third party providers. • Where applicable, share configuration records and information with Nationwide to support the completeness of the Nationwide Configuration Management System (CMS). • Ensure production or "live" services provided to Nationwide have no dependencies on any non-production components, so that insecure/unreliable service delivery and unplanned events may be avoided.
Monitoring Solutions **COBIT Ref: N/A**	• Ensure that all technology assets and related services are monitored to ensure any events are captured, recorded in operations logs, and acted upon - to prevent impact to business service provision. • Solution (including application, software and hardware) logs are retained for an agreed amount of time to allow for incident, security and problem management.
Managing Knowledge **COBIT Ref: BAI08**	• Ensure that knowledge levels, documentation and otherwise supporting information required to support services/solutions provided to Nationwide, is maintained.
Managing Incidents **COBIT Ref: DSS02**	• Operate a robust incident management process for the handling of incidents in relation to services or solutions being provided to Nationwide. • Have all relevant information recorded so incidents can be handled effectively, and are identified, recorded, prioritised, classified and resolved in accordance with the Service Level Agreements (SLA's) and Nationwide risk appetite. • Maintain full records relating to incidents for a minimum of 13 months. • Have a reporting process to immediately alert Nationwide of any incident, which may impact the ability to continue the provision of service. • Regularly review IT incidents with Nationwide.
Managing Problems **COBIT Ref: DSS03**	• Operate a regime/process of timely investigation into any problems which have been caused by technology incidents. This will include the identification and recording of such problems through root cause analysis and subsequent establishment and initiation of effective resolution plans to minimize the likelihood and impact of incident recurrence. • Ensure that there is proactive analysis of routine incidents/problems to identify and resolve the cause of common, high volume repeat incidents. • Ensure root cause determination and remediation for service impacting incidents is tracked to conclusion and consider 'read-across' issues in other technology services. This 'read across' includes reporting to Nationwide any incidents for other clients, which have the potential to also impact technology service provided to Nationwide.
Managing Services Requests **COBIT Ref: DSS02**	• Service requests are logged and categorised within an appropriate system • Requests are prioritised and managed, with appropriate authorisation workflows where required. • Have a full historical record of Service requests maintained and available for a minimum of 13 months.

Requirement	Description
Regulatory Compliance	Suppliers must: • Support Nationwide's compliance with relevant regulation such as FCA Handbook – SYSC 8 (Outsourcing), PRA Rulebook (Outsourcing), Information Commissioner's Office (ICO) requirements, including General Data Protection Regulation (GDPR), PRA Supervisory Statement 2/21 on Outsourcing & supplier Risk Management and forthcoming Consumer Duty (FCA). • Read, understand and comply with Nationwide's Supplier Code of Practice.
Negotiations	• Only undertake negotiations of service, contract and pay with Nationwide Procurement employees.
FSQS	• Join FSQS (Financial Services Qualification System) and fully complete the online questionnaire.
Information	• Provide accurate and complete information for due diligence and/or controls testing, such as: – Data Security certification – Regulatory permissions – Business Continuity plans – Operational controls – Sub-contractor governance arrangements
Governance & Oversight	• Report accurate, complete and timely Management Information in support of Service Level Agreements, actively participate in Performance and Relationship reviews as required.
Risks & Issues	• Immediately alert Nationwide to any issues, incidents or risks that may impact the provision of the service.
Material Changes	• Notify Nationwide of any material changes, including changes to the country from which the service is delivered and from where data is accessed/stored/used, move to Cloud storage or, introduction or change of a material/critical subcontractor.
Subcontractors	• Inform Nationwide of any sub-contracting arrangements put in place to support the Nationwide contract. • Provide accurate and complete information regarding those arrangements throughout the term of the contract. • Notify Nationwide of any changes to subcontractors (4th and 5th parties).

Vulnerability

The following requirements are applicable to suppliers who offer or administer products or services for Nationwide's customers on Nationwide's behalf.

A vulnerable is someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care. The risk of detriment arises not just from the customer's own circumstances but also from the interaction they are having with Nationwide and its suppliers. This includes change we may deliver that impacts an existing product or service. Examples of circumstances that may give rise to different or additional needs are:

Health Health conditions or illnesses that affect the ability to carry out day-to-day tasks	**Life Events** Major life events such as bereavement, job loss or relationship breakdown	**Resilience** Low ability to withstand a financial or emotional shock	**Capability** Low knowledge of financial matters or low confidence in managing money
Physical disability	Retirement	Inadequate (outgoings exceed income) or erratic income	Low knowledge or confidence in managing finances
Severe or long-term illness	Bereavement	Over-indebtedness	Poor literacy or numeracy skills
Hearing or visual impairments	Income shock	Over-indebtedness	Poor English language skills
Mental health condition or disability	Relationship breakdown	Low savings	Poor or non-existent digital skills
Addiction	Domestic abuse (including economic control)	Low emotional resilience	Learning difficulties
Low mental capacity or cognitive disability	Caring responsibilities		No or low access to help or support
	Other circumstances that affect people's experience of financial services e.g. leaving care, migration or seeking asylum, human trafficking or modern slavery, convictions		

Requirement	Description
Understand the Needs of Vulnerable Customers	Suppliers must: • Understand the nature and scale of characteristics of vulnerability that exist in the target market and customer base. • Understand the impact of vulnerability on the needs of customers in the target market and customer base, by asking what types of harm or disadvantage customers may be vulnerable to, and how this might affect the customer experience and outcomes. *The Importance:* • *Understanding the characteristics and needs of customers is key to providing good outcomes and preventing harm.* • *For example, failing to understand the needs of customers in the target market could result in inappropriate products being sold to customers resulting in poor outcomes.*
Skills and Capability of Staff	• Embed the fair treatment of vulnerable customers across the workforce. All relevant staff should understand how their role affects the fair treatment of vulnerable customers. • Ensure frontline staff have the necessary skills and capability to recognise and respond to a range of characteristics of vulnerability. • Offer practical and emotional support to frontline staff dealing with vulnerable customers. *The Importance:* • *It is essential that all employees understand the role they play and how they can prevent harm by recognising and responding to customers' needs.* • *For example, inability of staff to recognise signs of vulnerability could lead to a lack of appropriate support for the customer, causing harm.*
Product and Service Design	• Consider the potential positive and negative impacts of a product or service on vulnerable customers. Design products and services to avoid potential harmful impacts • Take vulnerable customers into account at all stages of the product and service design process, including idea generation, development, testing, launch and review, to ensure products and services meet their needs. *The Importance:* • *Products and services must be designed to ensure they are accessible and facilitate good outcomes thereby preventing harm.* • *For example, a customer who has lost their job could experience harm if they are unable to cancel a product they can no longer afford.*

Requirement	Description
Customer Service and Distribution	• Set up systems and processes in a way that will support and enable vulnerable customers to disclose their needs. Firms should be able to spot signs of vulnerability. • Deliver appropriate customer service that responds flexibly to the needs of vulnerable customers. • Make customers aware of support available to them, including relevant options for supplier representation and specialist support services *The Importance:* • *Flexible customer service is vital to ensuring all customers have a positive experience and to meet their individual needs.* • *For example, a customer may receive a poor outcome if they telephone to advise of a change in their circumstances and are told the process is to use another channel, such as online or visiting a branch.*
Communications	• Ensure all communications and information about products and services are understandable for customers in the target market and customer base. • Consider how to communicate with vulnerable customers, taking into consideration their needs. Where possible they should offer multiple channels so vulnerable customers have a choice. *The Importance:* • *When communicating with customers it is essential that we do so in a way that enables them to understand the message being delivered to prevent harm.* • *For example, a firm can cause harm if they are unable to provide a letter in a suitable format for a customer who is unable to read.*
Monitoring and Evaluation	• Implement appropriate processes to evaluate where the needs of vulnerable customers have not been met, so that improvements can be made. • Produce and regularly review management information, appropriate to the nature of the business, on the outcomes being delivered for vulnerable customers. *The Importance:* • *Monitoring and evaluation is key to understanding how we are meeting the needs of vulnerable customers and to make improvements where harm or poor outcomes and experience are identified.* • *For example, harm could be caused if data shows that customers with a characteristic of vulnerability are receiving lower levels of good outcomes than customers in standard circumstances and the firm fails to take action to understand the cause and remediate.*

Whistleblowing

At Nationwide we are committed to conducting our business with openness, transparency and integrity, and ensuring that concerns are appropriately investigated and responded to.

Nationwide has a Whistleblowing policy which sets out the process through which genuine concerns about potential or actual wrongdoing or misconduct by Nationwide's employees or its suppliers can be raised.

Requirement	Description
Customer Service and Distribution	Suppliers must: • Encourage employees, through communications and training, to raise concerns relating to wrongdoing, misconduct or inappropriate behaviours to their manager in the first instance. • If concerns relate to Nationwide, inform the Senior Relationship Owner to agree an approach to investigating and resolving the concern.
Communications	• Inform employees that in addition to their own internal procedures, employees engaged to work with Nationwide can also escalate their concerns related to Nationwide's business or their employees, directly through Nationwide's Whistleblowing arrangements. This can be done either confidentially or anonymously by: – Telephoning – 0330 460 5445 – Emailing - whistleblowingofficer@nationwide.co.uk; – Reporting via the Ethicspoint web portal on https://nbs.ethicspoint.com 24 hours a day, seven days a week – Writing to - Whistleblowing Officer, First Floor B, Nationwide House, Swindon, SN38 1NW; or contacting the FCA or PRA directly
Monitoring and Evaluation	• Ensure that nothing in the arrangement prevents or discourages employees, engaged to work with Nationwide, from choosing to make a protected disclosure via any of the above channels, including to the regulators, before following its internal arrangements. • Ensure contracts of employment, non-disclosure agreements and confidentiality agreements cannot prevent workers from reporting suspected wrongdoing, misconduct or inappropriate behaviours by Nationwide employees or its suppliers

Key Terms	
Protected Disclosure	A "qualifying disclosure" as defined in section 43B of the Employment Rights Act 1996, is in summary, a disclosure made in the public interest, of information which, in the reasonable belief of the worker making the disclosure, tends to show that one or more of the following ("failures") has been, is being, or is likely to be, committed: • A criminal offence. • A failure to comply with any legal obligation. • A miscarriage of justice. • The putting of the health and safety of an individual in danger. • Damage to the environment. • Deliberate concealment relating to any of the aspects listed above. It is immaterial whether the failure occurred, occurs or would occur in the United Kingdom or elsewhere, and whether the law applying to it is that of the United Kingdom or of any other country or territory.
Reportable Concern	A concern held by any person in relation to the activities of a firm, including: • Anything that would be the subject-matter of a protected disclosure, including breaches of rules. • A breach of the firm's policies and procedures. • Behaviour that harms or is likely to harm the reputation or financial well-being of the firm.

Updates to Policies

The policies are reviewed annually, or as the need arises to reflect internal or external changes. Key updates made since the previous version are detailed below.

Version	Date Published	Updates Since Previous Version
1.1	April 2024	Technology policy – terminology updated to reflect new internal requirements.
1.0	Oct 2023	N/A