Information Security Policy

For Suppliers and Senior Relationship Owners/Relationship Owners

Introduction

This guide sets out the Information Security requirements that are **applicable to Suppliers.**

These requirements support Nationwide in managing the Confidentiality, Integrity, and Availability (CIA) of Nationwide data.

Guidance for Suppliers considering doing business with Nationwide Building Society. More specific security requirements for each service will be assessed and agreed on a case-by-case basis.

All Suppliers must;

- Protect Nationwide information by restricting access to authorised users only using the principle of least privilege.
- Maintain accurate and up to date records of; and review user access rights to Nationwide Information.
- Identify information security risks and apply mitigating controls.
- Apply appropriate security controls in order to minimise risks of unauthorised access, disclosure, modification and loss of Nationwide information.
- Immediately alert Nationwide to any issues, incidents or risks.
- Minimise the business impact resulting from security incidents by conducting root cause analysis and remediation activity to reduce the risk of reoccurrence or similar incidents.
- Identify and implement the required security measures to protect Nationwide Information and Nationwide IT Systems from unauthorised access, disclosure, modification and loss.
- Maintain the availability of Nationwide Information and minimise the risk of system failures to Nationwide IT systems.
- Address known technical vulnerabilities within an appropriate timescale.
- Protect the confidentiality, integrity and availability of Nationwide Information when accessed, stored, managed, and processed by other authorised Suppliers.
- Protect Nationwide against malware and minimise business impact by responding to malware attacks.
- Detect any unauthorised access, modification, disclosure or deletion of Nationwide Information.

- Create and maintain a culture of information security where employees are educated in and understand and act upon responsibilities to protect Nationwide Information.
- Comply with relevant laws, regulations, and contractual requirements that relate to security.
- Securely recover, destroy and protect Nationwide Information as required.
- Embed security controls during the design, build, implementation and testing of Nationwide IT Systems.
- Protect Nationwide IT System from the risks associated with the internet connectivity (e.g. malicious code, breach)

Responsibilities of Senior Relationship Owners

Nationwide's Third Party relationship managers must:

- Implement appropriate Information Security oversight and governance, including monitoring of Service Level Agreements.
- Undertake ongoing operational due diligence to ensure that the Third Party continues to have the capability, capacity, and authority to provide the service to the standard required, and any risks identified are documented.