Nationwide
Physical Security Policy (Supplier)

Version – 1.0

Contents

1. Policy Objective

This external policy document sets out Nationwide Building Society's (Nationwide's or the Society's) approach to managing Physical Security Risk associated with third party suppliers. The Society operates a comprehensive Risk Management Framework through which all risks are identified and managed according to an assessment of severity (based on the combined impact of their individual impact and probability of crystallising).

The approach to identifying, assessing, monitoring, mitigating and reporting on individual risks is implemented through a suite of policies supported by standards and procedures. These have been designed to ensure adherence to the Society's Risk appetite and ongoing compliance with regulatory and other legal requirements as applicable to the Society.

The objectives of this policy are to:

- Define Physical Security Risk applicable to third parties;
- Document, at a high level, the minimum expected physical security standards required by third party suppliers;
- Ensure third party suppliers understand their obligations in respect of Physical Security Risk

1.1. Legal and Regulatory Requirements

There are no direct regulatory requirements for this policy; however, this policy forms a part of the systems, processes and arrangements that the Society has in place that are required under SYSC 3 (Systems and Controls).

2. Application

This policy is applicable to all applicable third parties that originate, receive, store, process or forward Nationwide Information, as defined by the Data Lifecycle[1].

2.1. Exclusions

Activity / Business Area	Exclusion	Rationale
No exclusions granted.		

2.2. Critical Control Activities

The below table provides a summary of the Critical Control Activities that are expected to be in place to ensure the confidentiality, integrity and availability of Nationwide physical assets controlled by third party suppliers

Ref	Control Activity	Summary of the nature of control
3.1.1	Physical Security - Policy	There must be a formally documented physical security policy with underpinning standards, processes and procedures with a nominated individual or role accountable for physical security.
3.1.2	Physical Security Risk Assessment	A Physical Security Risk Assessment must be carried out 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 must be applied to the facility and a Vulnerability Assessment undertaken to inform required physical security control measures. • As a minimum, the risk and vulnerability assessments are to be reviewed on a cyclical basis at pre-defined intervals (minimum annually), or in

[1] Create-Store-Use-Share-Archive-Destroy, as defined by ISC2

		response to received threat intelligence or as part of a Post Incident Review
3.1.3	Secure by Design	The development of a New Facility or transformation of an In-Use Facility must utilise a secure by design project lifecycle 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 must be undertaken to determine the required technical build configuration baseline standards (aligned with industry benchmarks). • Where non-conformances to the Build Standard are required, these are to be raised and logged as a Dispensation or Waiver and notified to Nationwide.
3.1.4	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 must provide a known level of security performance and be aligned with recognied industry benchmarks such as the Loss Prevention Certification Board (LPCB) or CPNI Catalogue of Security Equipment (CSE).
3.1.5	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) must be 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 must be retained for a period not less than 90 days. • Access permissions should be linked to the Joiners, Movers & Leavers process and should be promptly revoked when no longer needed.
3.1.6	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 to be registered and issued with a security pass which makes them easily identifiable as a vistor. • The visitor must be escorted by an employee of the 3rd Party when in the non-public space of the building / area and should return any security passes on exit from the premises. • The register of visitors is to be auditable and must be retained for a period not less than 90 days.
3.1.7	Incident Management	Physical Security incidents are identified, reported, and responded to in accordance with documented incident management procedures. Root cause analysis is performed to identify recurring issues that require risk management response or where risk appetite has been exceeded. Physical security incidents which have, or had potential to impact Confidentiality, Integrity or Availability of Nationwide physical assets must be notified to Nationwide.
3.1.8	Security Education and Awareness	Employees and contingent workers are provided with relevant and targeted security education, training and awareness based on an assessment of training needs on at least an annual basis.
3.1.9	Physical Security Event Monitoring and Incident Response	Facilities which are not 24/7 operational must incorporate an Intruder Detection System 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 should terminate 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 Detctions Systems, Automatd Access Control Systems) must be installed and maintained by an approved certified supplier (either SSAIB or NSI).

3. Policy Compliance

3.1. Non-Compliance and Requests for Dispensations, Waivers and Breaches

Compliance against this policy is required from the date of publication and support previous policy versions. Where policy requirements cannot be met, a request for a Dispensation or Waiver must be referred to Nationwide's Head of Security & Resilience Centre of Excellence via the Nationwide Third Party relationship manager(s).