Security and resilience

Protecting the things that matter most to our customers is our highest priority, this includes ensuring the security of our customers' money and data and providing resilient services. It's a priority we take seriously and something we continually invest in to ensure we are always evolving our security and resilience capabilities.

We are very proud of our security and resilience colleagues, who have won multiple awards for their work, including UK Security Team of the Year at the Computing Security Awards 2024. We ensure that there are colleagues working 24/7, 365 days a year, to keep Nationwide safe and secure. If you might be interested in joining them you can find out more about the team and see open vacancies here: Security & Resilience | Nationwide Careers.

Note: This area of our website offers information about some of the things we do as a responsible business. To report a security vulnerability visit Report a security vulnerability | Nationwide

Following the acquisition of Virgin Money on 1 October 2024, this policy statement is written on behalf of the Nationwide group, including Virgin Money.

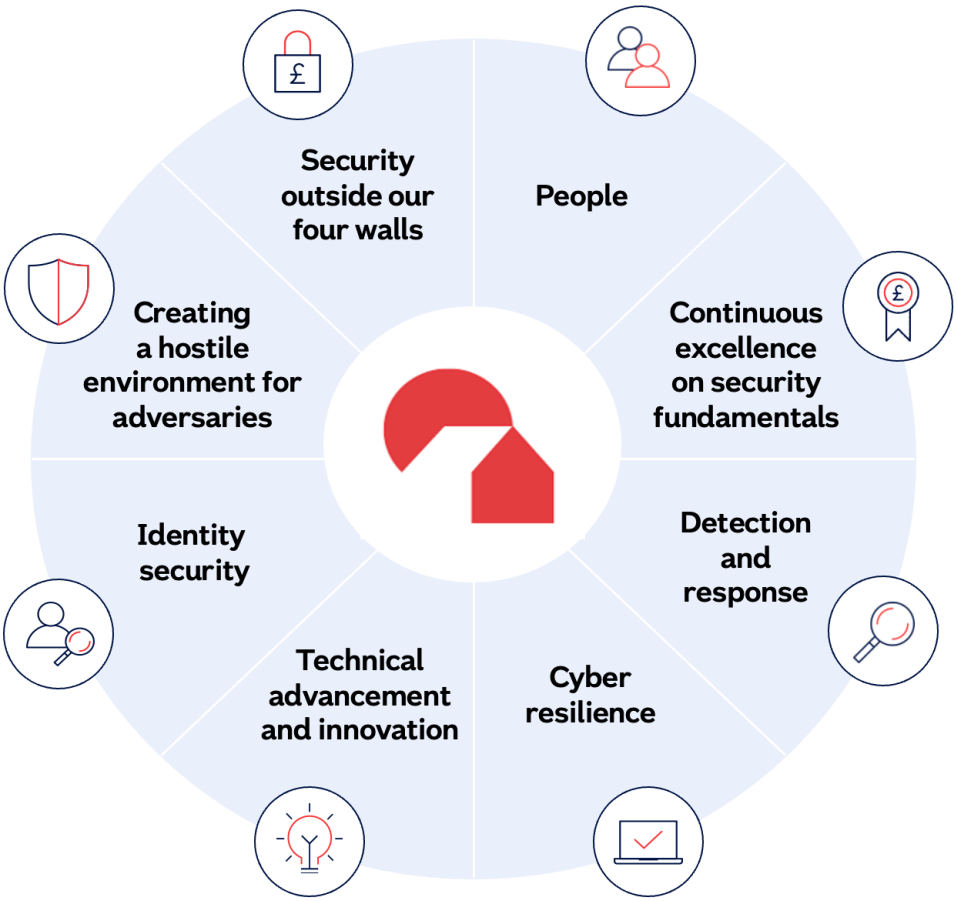
Our policies and practices

- We believe the foundations of strong security and resilience starts with our people, and our organisational culture prioritises both matters.
- Our policies and standards govern all business areas and outline how Nationwide protects the confidentiality, integrity and availability of information, systems and services.
- We make clear each colleagues' individual responsibilities for security and resilience. These responsibilities also extend to our third parties so that, collectively, we can deliver a secure and resilient operation for our customers.
- We continuously monitor the external landscape to identify potential security threats, whilst operating and maturing our key security controls to protect our customers and services. Significant effort is put into security risk management capabilities, with ongoing investment in the identification of risk, protection of data, detection and prevention of attacks and continued testing of response and recovery capability should an attack be successful.
- Testing of our multi-layered control approach is undertaken on an ongoing basis, including testing both the design of security controls and their operating effectiveness. Challenge and oversight is provided by our second line of defence teams and audit provided by our third line of defence teams. Our testing includes technical security testing using the same techniques seen in attacks elsewhere. We also conduct regular tests of cyber response strategies and security incident management procedures which could be invoked to maintain customer services should an attack be successful. This provides the Group with confidence in its controls and allows a better understanding of how to prevent future attacks, ensuring technical controls are constantly developed, resource is repositioned, and investment is allocated appropriately.
- Our cyber security approach is aligned to the National Institute of Standards and Technology (NIST) 'Cyber Security Framework' and we use this framework to assess our maturity, benchmark ourselves against our peers and identify opportunities for improvement.
- The accountable executive for cyber security is the Group Chief Security and Resilience Officer, who reports into the Group Chief Operating Officer. A separate Chief Information Security Officer is also dedicated to, and retains accountability for, cyber security at Virgin Money. The Board receives updates once a month on cyber security, with deep dives on cyber security once every six months. The Board are supported in discharging their accountabilities by a specialist Board cyber security advisor. Our external auditors, Ernst and Young, assess our security controls as part of their annual Group audit.

- We are committed to collective defence and preparedness in support of a secure and resilient UK economy and work alongside organisations such as, but not limited to, the UK Government, Law Enforcement, the Cyber Defence Alliance and SaferCash to achieve better security outcomes for Nationwide, for the UK economy and for the good of society.

Group security strategy 2026-2029

Our three-year Group Security Strategy runs from April 2026 – March 2029. It sets out the areas in which we will prioritise investment to support our management of security risk. Those areas are focused around eight pillars:



People risk Ensuring we have the best talent to defend the Society, fostering the right security culture, managing insider risk and keeping our colleagues safe.

Continuous excellence on security fundamentals Continually investing in delivering brilliant security basics because, whilst a constant challenge, it provides a disproportionate risk return on the investment if done well. Placing continued emphasis on ensuring the timeliness of patching, pushing for better on the reduction of our attack surface and continuous assurance over key security controls.

Detection and response Driving down further the mean time to detect and respond to security events across our different networks and systems.

Cyber resilience Ensuring that if other controls fail and an attack is successful, we have a tried and tested capability that can respond and recover services in a reasonable timeframe.

Technical advancement and innovation Keeping us ahead through preparing for foreseeable risks such as quantum computing and the offensive use of artificial intelligence. This will include through our work with Nationwide Ventures and investment in security research and innovation.

Identity security Ensuring effective controls against identity-based attacks. This includes enhancements to access management and the next step on our journey towards wider implementation of both a password-less organisation and zero-trust principles.

Creating a hostile environment for adversaries Prioritising preventative controls and making both our networks and associated systems less permissive environments for those that might wish to do us harm.

Security outside our four walls Managing supply chain risk and playing our part in wider UK security and resilience. We recognise our responsibility and the opportunity to work with partners to achieve better security outcomes for Nationwide, for the UK economy and for the good of society.