Information security

At Virgin Money, we take security extremely seriously and do everything we can to keep information safe. Customer trust is very important to us, so we work tirelessly to mitigate the risks of a cyber-attack, exposure or manipulation of confidential data and unauthorised access to information.

Customers' information is protected by regulation and legislation and every colleague has a responsibility to maintain the security of it – no matter the format.

We'll continue to develop our capabilities to mitigate information security risk in an environment where threats continue to evolve. We're keen to embrace new and emerging technologies while protecting the business from security threats like data loss, malware, phishing and hacking. Enhancing and investing in detective, preventative and responsive security controls is our clear ongoing strategy. Recognising the evolution of security threats and focusing on digital capabilities is more important than ever.

Keeping on the right track

Information security forms part of our wider Operational Resilience Strategy, which is to make sure we can always operate critical and important banking services. This is despite a backdrop of threats and adverse events in the environment.

We keep to strict information security standards and regularly have internal and external audits of our security controls. Independently, we test the effectiveness of our security controls using specialists to perform penetration testing and 'Red Team' exercises.

Our strategy is aligned to the NIST (National Institute of Standards and Technology) Framework and CIS (Center for Internet Security) Controls, which provide safeguards to mitigate risk. Our Information Security Policy Framework and supporting suite of standards set out our minimum control requirements. They're also aligned to ISO270001:2013 and CIS Critical Security Controls version 8.

Our SOC (Security Operations Centre) monitors security alerts 24/7. Robust protocols are in place to manage, respond and recover from any security event or incident.

Our Corporate Governance Framework oversees the management of information security risk in line with our risk appetite. We give quarterly reports to the Risk Committee and our Operational Resilience Strategy is reviewed by the Board of Directors yearly. Operational governance is provided across the Three Lines of Defence model, with continuous oversight and monitoring. This allows us to act quickly if we need to strengthen due to industry/regulatory requirements or in response to new security threats.

The standards we uphold

Our Information Security Policy Framework is in place to protect Virgin Money's reputation and safeguard our data assets, systems, services, customers, colleagues and shareholders. The framework prevents disruption to the business and minimises the impact of any information security incidents.

We do this by setting out our minimum control requirements to protect the confidentiality, integrity and availability of our information and information systems. Our framework has six Information Security Standards which apply to all job roles and a further nine standards relating to technology job roles. Here's a summary:

- Our colleague Terms and Conditions include complying with established Information Security Standards and procedures for their role.
- Colleagues must not share passwords, leave company devices unattended, use unauthorised software or keep company information in unapproved locations. They must also report any suspected breaches or incidents for investigation.
- We only allow authorised access to (and appropriate use of) our systems, giving colleagues the lowest amount of privilege needed to perform their job.
- Information must be classified, stored, transmitted and deleted appropriately. This is according to its level of confidentiality and the relevant regulatory standards at the time.
- There must be documented standards and procedures for the protection of information associated with critical IT infrastructure and security architecture.
- The management of vulnerabilities that have been identified must be mitigated in line with our minimum requirements.
- The design of our IT must have the appropriate service quality and mitigate against the identified risks of:
  - loss of service
  - degradation of service
  - financial loss
  - loss of reputation
- Third parties who process, store or transfer confidential business data or information relating to customers shall be assessed for information security competence. They'll also be subject to ongoing due diligence. The same goes for third parties who have access to our systems.

Our standards apply to the whole Virgin Money Group, including our employees, contractors, agency workers and directors. To help colleagues stay right up to date, they complete annual information security training. Plus, there's extra education for those who handle customer payments and our financial arrangements.

VM38270