Information Security Positioning Statement

Royal Mail Group

Our policies

Royal Mail Group manages information systems and processes to achieve an appropriate and pragmatic security risk profile, and to provide assurance to stakeholders and customers that data and information systems are protected from relevant security threats.

Royal Mail Group's information security policies and controls are aligned to the information security management system defined in ISO27001:2013 and the control objectives defined in ISO 27002:2013.

Security and privacy of customer data

Royal Mail Group has strict controls in place to protect the security and privacy of customer data as well as Royal Mail's corporate and operational data. These controls are designed into our services, IT solutions and infrastructure and maintained and supported via a set of strategic IT partners who are themselves ISO27001:2013 certified.

We have an Enterprise Security Architecture Framework which ensures that security controls applied to any system are commensurate with the criticality of the system, the confidentiality classification of the information, the trust classification of the processing environment and the access required to the information.

Changes affecting Royal Mail IT services and assets are assessed for their security and privacy impact prior to implementation. Based on the risk assessment, security controls are specified, solution designs reviewed and verified, and security testing is performed before releasing the changes to production. On a periodic basis, the security controls applied to critical business systems and IT infrastructure is assessed and where necessary, actions taken to ensure that they continue to comply with our policies.

Device and network security

Royal Mail user laptops and desktops are locked down by end point security solutions including malware protection, drive encryption, and centralised monitoring, with configuration policies globally enforced from a central IT authority. The networks are protected by malware protection, intrusion prevention and 24x7 security monitoring. All internal identities are managed centrally and access to business-critical applications are regularly reviewed for appropriateness.

Transmission of information

Our standard practice for transmission of information over public networks is to use secure channels such as HTTPS, SFTP or other secure message level and transport level security mechanisms. All supplier and external access to our network is via policy-controlled application and presentation level gateways situated at our network perimeters, which are monitored for intrusion and e-commerce fraud.

Employee vetting and training

Pre-employment background checks that meet the Baseline Personnel Security Standard are undertaken for all Royal Mail Group employees, who are also required to sign a Personal Declaration which outlines their obligations including confidential information and Data Protection. All contractors are also vetted prior to joining Royal Mail, and our strategic IT partners carry out equivalent vetting for their employees and contractors who are assigned to work with our systems or data. Appropriate standard confidentiality clauses are included in all Royal Mail Group contracts. Abuse or misuse of information or technical assets is considered a violation of our Code of Conduct, and can lead to dismissal of employees or termination of services from contractors. They may also give rise to criminal and civil proceedings.

All personnel undertake annual mandatory training. Additionally we regularly promote cybersecurity awareness initiatives and run phishing simulation campaigns. Our goal is to empower our employees, equipping them with the knowledge to make informed decisions, and skills to protect our sensitive data and systems.

Disclaimer

This statement has been prepared by Royal Mail Group solely to provide general information. Royal Mail Group has made reasonable efforts to ensure that it is accurate at the time of production. This statement and its contents do not constitute a commitment by Royal Mail Group to continue any of the practices or procedures described in the statement, or to notify any party of changes to the practices or procedures described, either in advance of or following such changes