



Information Security Schedule For Contractors

September 2004

Document Details

Owner: Director of Information Security
Date of this document: September 2004
Version: 1.0
Status: Final
Classification: Public

© Royal Mail 2004

Royal Mail is a trading of name Royal Mail Group plc. Registered number 4138203.
Registered in England and Wales. Registered office: 148 Old Street, LONDON, EC1V 9HQ

Information Security Schedule For Contractors

CONTENTS

1	Purpose and Scope of Information Security.....	1
2	Contractors Obligations.....	1
2.1	Compliance with legal and contractual requirements.....	1
2.2	Design of Information Systems.....	1
2.3	Access to Royal Mail Information Systems & Applications.....	2
3	Management of Information.....	2
3.1	Data protection.....	2
3.2	Personnel security.....	2
3.3	Physical & environmental security.....	3
3.4	Access control.....	3
3.5	Appropriate Use of Royal Mail Systems.....	3
3.6	Incident response.....	4
3.7	BS7799.....	4
3.8	Supplier Management.....	4

Information Security Schedule For Contractors

1 Purpose and Scope of Information Security

The purpose of Information security is to safeguard the reputation of Royal Mail, enhance the value of its brands and help to optimise the management of risks.

Royal Mail security requirements are based on ISO/IEC 17799:2000 Code of Practice for Information Security Management, which defines information security as the preservation of:

- confidentiality: ensuring that information is accessible only to those authorised to have access;
- integrity: safeguarding the accuracy and completeness of information and processing methods;
- availability: ensuring that authorised users have access to information and associated assets when required.

A number of Royal Mail information systems have been certified against the Code of Practice, therefore Contractors' compliance with this schedule is essential.

2 Contractors Obligations

2.1 Compliance with legal and contractual requirements

All Contractors to Royal Mail must ensure that their people, systems and processes comply with the contractual requirements and relevant legislation which includes:

- Data Protection Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Companies Act 1985
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Postal Services Act 2000

2.2 Design of Information Systems

Appropriate information security controls must be implemented to protect information assets from internal and external security threats, whether intentional or accidental. Security controls must be consistent with Royal Mail Group policies and standards.

To maximise security benefits, decisions concerning security controls must be taken at each point in the system or application life cycle, i.e. during Requirements Definition, Technical Design, Development, Test, and Deployment.

Security requirements must always be addressed in the Requirements Definition phase of a project and should incorporate a risk assessment to ensure that security controls reflect:

- the information classification of data accessed or generated

Information Security Schedule For Contractors

- the levels of trust in the identity associated with the members of the user community
- system availability requirements.

Where security has not been addressed in the requirements phase the system or application will be non-compliant and will not be permitted to enter the deployment phase until it is secure.

2.3 Access to Royal Mail Information Systems & Applications

Contractors will only be granted access to Royal Mail information systems and applications where the Royal Mail has defined a clear requirement for access. Contractors accessing Royal Mail systems and applications will be subject to the same terms and conditions of access as Royal Mail employees. Misuse of Royal Mail Group information systems will lead to termination of the contract and possible legal action against the contractor.

3 Management of Information

Contractors must:

- ensure that information is only accessible to those authorised to have access
- safeguard the accuracy and completeness of information and processing methods
- ensure that authorised users are able to access to information and associated assets when required

The individual components of these requirements are:

- Data Protection
- Personnel security
- Physical and environmental security
- Access control
- Incident reporting and use of Royal Mail systems

3.1 Data protection

All Contractors dealing with personal data about living individuals on Royal Mail systems must comply with the provisions of the Data Protection Act 1998.

To prevent the misuse of personal data, the Act puts safeguards in place to protect individuals and contains eight principles that deal with matters such as data collection, disclosure, retention and accuracy.

Individuals have the right to see their personal data, to have copies of that data and to have the data corrected or erased where it is inaccurate.

3.2 Personnel security

Royal Mail requires the Contractor to:

- Provide assurance that employees have proven identities, adequate character references and that curriculum vitae and qualifications are genuine

Information Security Schedule For Contractors

- Provide assurance that employees are trained in security procedures and the correct use of information processing facilities to minimise possible security risks
- Ensure that employees are aware of the need to report security incidents through the appropriate management channels
- Maintain a disciplinary process for employees who have violated security policies and procedures
- Monitor system usage and maintaining audit logs to detect and report on breaches of this schedule or misuse of Royal Mail Systems and information.

3.3 Physical & environmental security

The Contractor must ensure that the security of premises and the working environment for the protection of business assets and employees has been adequately addressed. Basic security controls to be deployed include:

- secured perimeters and entry points
- secured facilities for the protection of valuable, critical or sensitive assets from theft or disaster
- the siting or protection of equipment to minimise risks from hazard or unauthorised access
- clear desk and clear screen policy
- controls to prevent unauthorised removal of equipment

3.4 Access control

If a Contractor requires access to Royal Mail systems as part of the obligations of the Agreement the formal approval process must be followed and the Contractor must ensure that only named personnel have access to the system.

For each access the security risks and need for any specific restrictions, security education and additional controls must be considered by both Royal Mail and the Contractor and appropriate measures implemented.

Access to any physical information held by the Contractor must be protected by the methods given above XX and information should be returned to Royal Mail on the expiry or termination of the Contract.

3.5 Appropriate Use of Royal Mail Systems

Royal Mail information systems may not be used to:

- to undertake activities detrimental to the reputation or business interests of Royal Mail Group plc
- to express unauthorised views or make commitments that could appear to be on behalf of Royal Mail Group plc
- to copy, distribute or receive copyrighted or confidential materials without the authority of the owner
- in a way that adversely affects the work performance
- to further the interests of any non-Royal Mail business enterprise or other organisation, in connection with any self employment beyond the business, or on behalf of or in the interests of any non-Royal Mail employee

Information Security Schedule For Contractors

- to undertake activities, make statements, deliberately visit web sites or disseminate or retrieve information or software containing material of an offensive, sexual or discriminatory nature based on sex, race, sexual orientation, age, disability, national origin, religious or political beliefs.
- to transmit or store messages or material employing language or including images that are obscene, sexually oriented, derogatory, offensive, threatening, insulting, harassing or harmful to recipients
- to deliberately visit web sites or contribute to News Groups that advocate illegal activity
- to initiate or participate in the sending of chain letters, 'junk mail' (unsolicited commercial electronic mail), 'spamming' (sending unsolicited messages indiscriminately to multiple mailing lists, individuals, or newsgroups) or other similar mailings
- to transmit messages or material that are damaging to the reputation of Royal Mail Group plc, or that of its products or services, or are libellous of any other person's or company's reputation, products or services
- to transmit messages or material that solicit or promote a religious, charitable, political or other non-business related cause, unless authorised by the company (arrangements remain unchanged for sponsorship/collections for charities undertaken by individuals and involving Royal Mail employees)
- to obtain or disseminate unauthorised software that could put the security of the Royal Mail network at risk

Contractors must comply with this if they have access to Royal Mail systems as part of their obligations to the agreement between themselves and Royal Mail.

3.6 Incident response

If there is a loss of information or a breach of the security of the information held by the Contractor as part of the obligations of this contract this must be communicated at once to the Royal Mail Representative detailed in the General Schedule of the Agreement.

3.7 BS7799

BS7799 accredited certification is the preferred method for demonstrating compliance with ISO/IEC 17799 : 2000 Information Technology – Code of Practice for Information Security Management. Royal Mail currently holds this accreditation. The supplier will implement all necessary measures to ensure that Royal Mail maintains this certification.

3.8 Supplier Management

Contractors activities to comply with this schedule will be managed via the supplier management meetings as detailed in the supplier management schedule.