RMG00000318

intouch

INTOUCH MANAGEMENT COMMUNICATION SYSTEMS LIMITED SERVICE AGREEMENT

InTouch Management Communication Systems Limited of Blythe Valley Innovation Centre, Blythe Valley Park, Shirley, Solihull B90 8AJ, United Kingdom ("InTouch") and Royal Mail Group Limited, 100 Victoria Embankment, London EC4Y 0HQ United Kingdom (the "Client"), hereby agree as follows:

Definitions

Client's Personnel means the employees, staff, agents, sub-contractors and advisors of the Client and its direct and indirect subsidiaries including General Logistics Systems B.V. For the avoidance of doubt, Client's Personnel shall include Post Office Limited sub-postmasters.

Effective Date means 02nd August 2010

1. Services

1.1 InTouch will provide the Client with the following services ("The Services"):

(a) InTouch will provide access 24 hours a day, 365 day a year access to all of the Client's Personnel (the "Client's Personnel") in the United Kingdom as set out in Schedule A to (i) call handlers (ii) its secure web reporting facility and (iii) its automated 'SpeakUp' IVR system. Telephone access is via a free phone number. The service is intended to be used for the recording of the Client's Personnel's concerns of a "whistleblowing" nature and other malpractice issues, including fraud, financial irregularities and HR concerns.

(b) InTouch will agree with the Client a script that callers will hear when they contact the IVR system. InTouch will agree with the Client the text that will be shown on the web reporting pages. InTouch will further agree with the Client the framework of

RMG00000318

questions to be used by the call handlers. The Client can amend the script, text on the web reporting page and framework of questions at any point during the term at no additional cost.

(c) InTouch will forward as appropriate the call handlers' notes or verbatim transcripts of the concerns raised by its Client's Personnel to the Client's nominated contacts usually by the next working day after receipt. Messages will normally be forwarded by e-mail and will always be encrypted through PGP encryption.

(d) The Client will receive all messages left by employees. InTouch does not filter messages on behalf of the Client.

(e) The Client is able to respond to anonymous messages as designated by unique case numbers via the InTouch systems to provide feedback or ask follow-up questions of the Eligible Employee.

(f) A monthly summary of the type and number of messages received will be provided to the Client's nominated contact(s) by InTouch within 10 working days from the end of each month in Excel format stating date and time of call, unique case number, format of complaint (telephone, email) and type of complaint.

(g) InTouch will provide a named point of contact to account manage the service and provide ad hoc information as and when requested by the Client.

(h) The parties will meet on a three monthly basis at a location of the Clients choice, to discuss the Services.

(i) Intouch will meet the service levels as further detailed in Schedule B.

(j) InTouch will comply with Royal Mail policies and best practice as detailed in Schedule C.

1.2 InTouch shall perform the Services with such care, skill and diligence and to such high standard of quality as it is reasonable for the Client to expect in all the circumstances.

1.3 The Services shall accord with the terms of any statute, act, instrument, regulation, directive, decision and code of practice or other measure at any time in force and affecting such Services.

RMG00000318

1.4 InTouch represents and warrants that the assurances given in Schedule B under 'Agreed Service Level' will remain true and accurate during the term of the Agreement.

2. Promotion

InTouch will provide the Client with generic information taking into account local legal requirements to help the Client develop materials necessary to promote access by the Client's Personnel. The Client is responsible for any personalisation of such materials and can choose to promote the service under the name 'InTouch', 'SpeakUp' or any other name of their choice.

3. Caller Anonymity

InTouch will not attempt in any way to identify any user of the Services or trace any telephone call. It will not provide the Client with any records from which the identity of any anonymous user may be determined. However in the case of potential unlawful acts or threats, this clause does not apply and InTouch will provide a Client with all information in its possession

4. Confidentiality

4.1 InTouch will keep confidential and will not disclose to any other person, firm or corporation other than the Client, any information it receives by virtue of its provision of the Services (including, without limitation, any information concerning the Client and the content of any messages InTouch receives concerning the Client) (the "Information"). InTouch shall use the Information solely for the purpose of providing the Services to the Client and not for any other purpose.. InTouch may create compilations and reports to the Client of generic information in formats which will not allow matching of calls with particular Client's Personnel.

4.2 InTouch shall not disclose the Information directly or indirectly to any person except those of its officers, employees and the call handling partner Personal Performance Consultants UK Limited, who have a need to know (and only to the extent that each has a need to know) for the purposes of providing the Services and who are aware that all Information must be kept confidential.

4.3 InTouch shall securely return the Information, all copies, notes and records of the Information to the Client and securely erase and destroy the Information from any computer or other device within the control of InTouch immediately upon request and shall confirm to the Client in writing that InTouch has complied with this clause 4.3 in its entirety.

RMG00000318

4.4 InTouch shall not advertise or otherwise publicise its relationship with the Client or the Client's group of companies in any way (except with the prior written consent of the Client).

4.5 All communications between InTouch and Royal Mail will be secure and encrypted through PGP encryption.

4.6 InTouch shall protect the confidentiality of the Information both from internal and external threats, by providing the Services with such care, skill and diligence and to such high standard of quality as it is reasonable for the Client to expect in all the circumstances.

4.7 InTouch shall indemnify and keep the Client and Client Personnel indemnified against any and all loss incurred or suffered by the Client howsoever arising as a result of, or in connection with, a breach or failure by InTouch to comply with its obligations in this clause 4.

5. Payment Terms

5.1 The fees for the Services described in this Agreement are made up of an initial set-up fee and a recurring annual fee. The set-up fee is invoiced on the date the Agreement is signed. The annual fee is invoiced on the Effective Date and annually thereafter. The fees for the Services and the Effective Date are set out in Schedule A.

5.2 Subject to InTouch satisfactorily performing its obligations under this Agreement, the Effective Date is to be a date not later than 120 days after the Agreement is signed.

5.3 The Client shall pay all undisputed invoices issued in accordance with this Agreement within 45 days of the date of invoice

5.4 The Charges shall be as stated in this Agreement and, unless otherwise so stated, shall be exclusive of any applicable value added tax (which shall be payable by the Client subject to receipt of a VAT invoice).

6. Term and Termination

6.1 This agreement will commence on the Effective Date as set out in Schedule A and will continue until terminated in accordance with this clause.

6.2 Either the Client or InTouch may terminate this agreement immediately upon:

RMG00000318

6.2.1 a material breach by the other upon 7 days' written notice. The parties agree that any breach of clause 4 by InTouch shall be deemed a material breach; or

6.2.2 the other party ceasing or threatening to cease to carry on business or is unable to pay its debts as they fall due for payment.

6.3 The Client may also terminate this Agreement immediately upon any breach of clause 4 by InTouch.

6.4 Either party may terminate the agreement at any time on giving 90 days' written notice. Any amounts paid in advance by the Client shall be pro-rated such that the Client shall be reimbursed upon demand any amounts paid in respect of a period falling after the date of termination.

7. Liability of InTouch

The Client agrees that the amount of damages due from InTouch shall not exceed three times any fees paid or payable to InTouch under this agreement in the twelve month period immediately preceding any breach.

8. Governing Law

This agreement is governed by English law and the parties agree to submit to the non-exclusive jurisdiction of the English Courts.

9. Contracts (Rights of Third Parties) Act 1999

9.1 InTouch acknowledges that it may provide Services under this Agreement on behalf of other companies within the Client's group and therefore all such companies shall each have the benefit of the Client's rights under this Agreement and shall have the right to enforce such rights in accordance with the provisions of the Contracts (Rights of Third Parties) Act 1999. Except as stated in this clause 9, the parties to this Agreement do not intend that any of its terms will be enforceable by virtue of the Contracts (Rights of Third Parties) Act 1999 by any person not a party to it.

9.2 The parties reserve the right to rescind or vary this Agreement or vary any term of it without the consent of any of the Client's group companies.

10. Sub-Contracting

RMG00000318

10.1 InTouch shall not sub-contract, assign or otherwise transfer part or all of this Agreement or the Services without the prior written consent of an authorised representative of the Client.

10.2 Where callers choose to speak to a Service Representative this part of the service is provided by Personal Performance Consultants UK Limited ("PPC") whose address is set out in Schedule A.

10.3 InTouch shall remain at all times liable to Royal Mail for the acts and/or omissions of PPC or any other sub-contractor.

11 Audit

11.1 The Client or any third party appointed by the Client or any regulator with authority over the Client ("Inspector") may enter upon InTouch's premises and any property used by InTouch to provide the Services to verify compliance by InTouch with its obligations under this Agreement, in particular InTouch's compliance with the policies set out at Schedule C. The Inspector shall be entitled to have access to all files, records, personnel and data relevant to the operation of this Agreement by InTouch.

11.2 InTouch shall procure that satisfactory facilities (including copying facilities) are made available to the Inspector and that reasonable assistance (including access to relevant personnel) is given.

12. Severance

12.1 If at any time any one or more of the provisions hereof is or becomes invalid, illegal or unenforceable in any respect under any law, the validity, legality and enforceability of the remaining provisions hereof shall not be in any way affected or impaired thereby.

12.2 If any such provisions shall be found to be invalid or unenforceable but would be valid if some part thereof were deleted or the period or area of application reduced, such provisions will apply with such modification or modifications as may be necessary to make them valid and effective.

13. Reputation

InTouch shall not do or omit to do anything which might damage the reputation and/or goodwill of the Client (or any member of the Client's group of companies).

RMG00000318

14. Provision of Information

InTouch shall provide such management information as the Client may require from time to time in respect of the Services.

15. Amendments

No alteration, waiver or modification of this Agreement shall be binding on the Client unless made in writing and signed by an authorised representative of the Client.

16. Notices

Any notice or other communication required to be given by InTouch under this Agreement shall be addressed to *(insert Client's address)* and may be personally delivered (such term for the purposes of this clause to include delivery by courier)

IN WITNESS WHEREOF the duly authorised representatives of the parties hereto have signed this Agreement the day and year first above written.

..GRO.....

INTOUCH MANAGEMENT COMMUNICATION SYSTEMS LIMITED

(Duly authorised signatory)

NAME: JOHN WILSON

TITLE: Director

.....

Royal Mail Group Limited

(Duly authorised signatory)

NAME: GRO

TITLE: T.J. BULLOCK

HEAD OF TACTICAL SOURCING

RMG00000318

SCHEDULE A

The Charges will be reviewed on an annual basis.

1. Fee Structure (exclusive of VAT)

Fees are based on approximately 180,000 employees nationwide across the UK

Initial System Configuration:
(a) Programming of the telephone and web platform, scripting customised web intake and telephone prompts; translation work; personalisation of web and telephone intake for each country / language/ regulatory combination

(b)
Project management: orientation of call handlers; advice on suitable promotional campaigns; supplying generic artwork if required

For (a) and (b) a one off set fee of £1,650 will be paid

(i) Annual Service Fee
Fully inclusive of freephone charges and ongoing account management; translation of employees' messages as required; regular management information; legal and best practice updates

A fixed fee of £32,400 will apply for up to 400 calls. For any additional calls the following cost per call will apply.

Total number of calls per year	Cost per call
401-500	£45
501-1000	£36
1001-1500	£27
1501-2000	£21
2001+	Free of charge

Any original design, print and production costs of promotional items is at extra cost

Subject to VAT at the standard rate

RMG00000318

2. Countries and languages

Access to the InTouch call handling, web and IVR Services is from the following countries and in the following languages:

Country	Language
United Kingdom	English

3. PPC

Personal Performance Consultants UK Limited
4200 Nash Court
Oxford Business Park
Oxford
OX4 2RU

SCHEDULE B

Service Level Agreement

Page	Required Service	Description of risk and issue to be addressed	Agreed Service Level
1	Security of data	Overarching question about the data. Do you store anywhere the name of the company? Do the paper and computer records contain the name of the company or just an anonymous reference to it?	Intouch to set up their systems so that we do not use the name Royal Mail and instead use a pseudonym. The transcriptions of reports can contain headers which are similarly anonymised but if there is specific mention of a location or individual then it would not seem sensible or practical to redact these references.
1	Paper records: All clients - A paper copy of each message is retained for one month to assist the reporting process. During the next month the paper records are shredded as each client's monthly report is produced. Documents are shredded in a cross cut shredder in our office. Paper copies of regular monthly or weekly summaries may also be retained for one month and then shredded.	Where are the paper records kept? Do you use Safes?	Paper records are kept in a fire proof safe overnight.
1	Computer records: Whistleblowing clients -	How are the computer records deleted?	Files are deleted and erased using a secure shredder utility. Unused disk space is securely

RMG00000318

Page	Required Service	Description of risk and issue to be addressed	Agreed Service Level
	Client messages in Word and sound files of messages are retained for 2 months and then deleted. On a client by client basis we may agree to delete sound files and Word documents as soon as a client acknowledges receipt of a message.	How are they removed from backups?	wiped on a weekly schedule. Backups of files made prior to deletion are retained for one week on password protected media with restricted access to restore files.
1	Reports for whistleblowing clients will contain anonymised, brief summaries of messages received so that individuals mentioned in the summaries cannot be identified. These summaries will be retained for 12 months.	Do the reports contain Information about the company the whistleblower works for?	Yes, in so far as the information is required to enable Royal Mail to appropriately investigate the reported incident
2	Computer back ups: These are carried out on a daily basis and the tapes are retained off site in a safe in the home of one of the Company's Directors.	Do the computer backups contain word and sound files? Are they encrypted? If so how?	Identifiable word and sound files are backed up on password protected media.
2	Access to office pc's: All pc's and servers are password protected. As all office based staff have a need to access all the files the passwords on each pc or server are known to all staff.	Access to Office PC's How often are the passwords changed? Are the pcs accessible remotely from staff? Does each user have a unique ID and password? Do you change the shared password/accounts when a user leaves?	Passwords for office PCs are changed every three months and when a member of staff leaves. Staff do not have remote access to their PCs or files stored on shared network drives. Usernames and passwords are configured and different for each user. Internal User-IDs of former staff are deleted or disabled.
2	McAfee VirusScan Enterprise is in use on all our systems. The Firewall has the latest updates installed on a daily basis.	Who manages the firewalls? Do you have a dedicated team? How do you handle security incidents?	Shared passwords permitting remote access to the web reporting application are changed every three months or at the time staff leave. Network Firewalls are Netgear "Prosafe" units with the latest software updates installed. These are managed by external IT support staff and no internal staff have access to their configuration. There is no UPNP support for firewall configuration from client PCs. McAfee Enterprise Anti-Virus is monitored internally on a weekly basis to ensure systems are up to date and updated with the latest patches as they are released and stable. Security incidents are minimised by maintaining good user practices and very restricted personal use of IT systems, coupled with appropriate

RMG00000318

Page	Required Service	Description of risk and issue to be addressed	Agreed Service Level
			business security measures, which are monitored and updated regularly.

RMG00000318

SCHEDULE C

Client Policies with which InTouch must Comply

1) Third Party Services Policy

Purpose of the policy

To ensure that the Royal Mail Group information security requirements are identified, agreed and maintained whenever services encompassing Royal Mail Group information or information systems are entrusted to a third-party.

Risks and implications

A failure to comply with this policy could expose the Royal Mail Group to inadequate assessment of the information risks associated with outsourcing a particular function of the business, incorrect identification of the controls required to manage these risks and insufficient monitoring and review of controls in the outsourced function.

Furthermore, a failure could constitute a breach of our legislative, regulatory and/or contractual requirements, including the Data Protection Act (1998).

Who does this policy apply to?

All Royal Mail Group employees who have the authority and responsibility to prepare and engage the organisation in third-party service contracts.

Scope of the policy

This policy applies to all Royal Mail Group contracts with third-party and outsourced service providers, suppliers, vendors and resellers.

Policy statements

It is the policy of the Royal Mail Group that:

1.2a All third-party contracts must be approved by the Royal Mail Legal department and include the following:

- the determination of acceptable service levels and availability;
- the right for the Royal Mail Group to physically and logically audit the third-party environment for the appropriateness and effectiveness of the security controls applied to the Royal Mail Group's information;
- the need for the third-party to implement the Royal Mail Group policies for all services provided to the Royal Mail Group;
- documentation of physical and logical controls employed by the third-party to protect the confidentiality, integrity and availability of the Royal Mail Group information and information systems;
- the determination of all legal and regulatory requirements including privacy and data protection;
- the need for the third-party to uphold the confidentiality of all Royal Mail Group information and information systems; and
- agreement that the third-party must maintain and periodically test the agreed security controls and report the results to the Royal Mail Group.

1.2b Royal Mail Group contract managers must be assigned the responsibility of managing the relationship with the third-party and ensuring that the third-party is enforcing the requirements specified in the contract.

RMG00000318

1.2c All third-parties must be required to immediately inform the Royal Mail Group contract manager of any security breaches, including unauthorized access to or compromise of the Royal Mail Group information or resources.

1.2d The ownership of any software developed by third-parties, on behalf of the Royal Mail Group, must be defined in the contract agreement.

1.2e Formal exchange agreements must exist between contracted third-parties and the Royal Mail Group for exchanging information.

1.2f Risk assessments must be performed whenever the third-parties make significant changes to the services and products delivered to the Royal Mail Group (e.g. introduce new technologies, new development environments and tools, new hosting facilities).

1.2g All physical and logical access to the Royal Mail Group information and information systems must adhere to the *Third-Party Access Policy*.

1.2h All third-party agreements must specify the requirements for transitioning information and information systems back to the Royal Mail Group to ensure that the appropriate level of security is maintained.

Compliance

Group Information Security will regularly assess for compliance against this policy. Any violation of this policy will be investigated and if the cause is found due to wilful disregard or negligence, it will be treated as a disciplinary offence. All disciplinary proceedings are coordinated through the Human Resources Department.

The Royal Mail Group reserves the right to amend this policy at any time and will publish updated versions to all staff.

Associated policies, guidelines and procedures

Policy Statement Ref.	Title of policy, guidelines or procedure
1.2a-1.2h	*Guidelines for Third-Party Services*
1.2g	*Third-Party Access Policy*

ISO 27002 controls addressed

A6.1.5, A6.2.1, A6.2.3, A10.2.1, A10.2.2, A10.2.3, A10.8.2, A12.5.5

2. Incident Management Policy

Purpose of the policy

To minimise the impact caused by information security incidents and malfunctions on information systems operated by or on behalf of the Royal Mail Group.

Risks and implications

A failure to comply with this policy could expose the Royal Mail Group to a prolonged impact arising from unreported or unmanaged information security incidents, an inability to collect and present legally admissible evidence and a breach of our legislative, regulatory and/or contractual requirements, including the Data Protection Act (1998) and PCI DSS.

Who does this policy apply to?

RMG00000318

All Royal Mail Group employees and all agents, contractors, consultants and business partners (hereafter referred to as 'users') handling Royal Mail Group information.

Scope of the policy

All information and information systems developed by or on behalf of Royal Mail Group, including joint venture companies and outsourced units.

Policy statements

It is the policy of the Royal Mail Group that:

8.1a All users must immediately report all information security incidents and events, or suspected information security weaknesses, to the appropriate management channels and/or the Royal Mail Group IT Helpdesk.

8.1b It is prohibited for users to test any information security weaknesses without the cooperation and involvement of Group Information Security.

8.1c All users must not disclose the details of any information security incidents to non-contracted third parties without explicit management authorisation.

8.1d Formal information security incident management procedures, including a method of incident categorisation based upon type, impact and severity levels, must be developed to ensure a timely, effective, and managed response to information security incidents.

8.1e These procedures must explicitly define the roles and responsibilities assigned to manage information security incidents (e.g. technical response teams, management, business analysts, Legal, HR and Communications representatives) as well as reporting and escalation procedures.

8.1f All files collected as evidence in the investigation of a security incident must be collected and secured using appropriate forensics procedures, ensuring a chain of custody. Group Information Security is responsible for performing or coordinating any collection of information for use in an investigation.

8.1g All reports of security incidents or violations of information security policy must be documented and include a review process in order to identify root causes, define any required preventative improvements and coordinate appropriate training and awareness sessions within the Royal Mail Group.

Compliance

Group Information Security will regularly assess for compliance against this policy. Any violation of this policy will be investigated and if the cause is found due to wilful disregard or negligence, it will be treated as a disciplinary offence. All disciplinary proceedings are coordinated through the Human Resources Department.

The Royal Mail Group reserves the right to amend this policy at any time and will publish updated versions to all staff.

Associated policies, guidelines and procedures

Policy Statement Ref.	Title of policy, guidelines or procedure
8.1a-c	*Guideline for Reporting Information Security Incidents*

ISO 27002 controls addressed

A13.1.1, A13.1.2, A.13.2.1, A.13.2.2, A.13.2.3

3) User Access Management Policy

RMG00000318

Purpose of the policy

To ensure that the user access control requirements to the Royal Mail Group information and information systems are appropriately defined.

Risks and implications

A failure to comply with this policy could expose the Royal Mail Group to accidental or deliberate misuse of information systems, breaches of confidentiality, malicious or accidental corruption of data, theft of intellectual property and a breach of our legislative, regulatory and/or contractual requirements, including the Data Protection Act (1998) and PCI DSS.

Who does this policy apply to?

All Royal Mail Group employees and all agents, contractors, consultants and business partners (hereafter referred to as 'users') requiring business access to the Royal Mail Group information and information systems.

Scope of the policy

All information and information systems developed by or on behalf of Royal Mail Group, including joint venture companies and outsourced units.

Policy statements

It is the policy of the Royal Mail Group that:

6.2a All access to the Royal Mail Group information systems must be controlled by an approved authentication method supporting a minimum of a user ID and password combination that provides verification of the user's identity.

6.2b All users must be limited to only one user account for each individual information system for non-administrative purposes.

6.2c All individual user IDs must be unique for each user and never duplicated.

6.2d Shared user IDs must only be used if there is a clear business case and must be approved by the Information Owner and Group Technology.

6.2e Formalised user account management procedures must be implemented for user registration, modification and de-registration on all Royal Mail Group information systems. These user account management procedures must also include processes for monitoring redundant and inactive accounts.

6.2f Information Owners must authorise all user access granted to and revoked from the Royal Mail Group information systems using the approved user account management procedures.

6.2g All user access rights to the Royal Mail Group information and information systems must be limited to the minimum access rights necessary for the user to fulfil their business responsibilities as determined by their role.

6.2h All user access rights to the Royal Mail Group information and information systems must be reviewed by the Information Owners on a periodic basis.

6.2i All user accounts that have not been accessed for 90 days must be automatically disabled. The Information Custodians must inform the Information Owner of inactive accounts at regular intervals.

6.2j All users that have access to privileged accounts must have their own individual accounts for normal business use. Shared privileged accounts must never be logged into directly if their usage can not be tracked.

6.2k All administrator and privileged accounts must be based upon job function and authorised by the Information Owner prior to access being given. All changes to privileged accounts must be logged and periodically reviewed.

6.2l All default system and vendor passwords must be changed immediately following installation.

RMG00000318

6.2m All Royal Mail Group information systems must support strong password management techniques (e.g. length, complexity, aging, history, account lockout) in accordance with the *Guidelines for User Access Management*.

6.2n All Royal Mail Group information systems must technically force new user accounts to change the initial password upon first use to a strong password and thereafter every 90 days in accordance with the *Guidelines for User Access Management*.

6.2o Formalised procedures for the secure transmission of new and reset passwords that includes an acknowledgement of receipt must be established.

6.2p Passwords must never be shared, written down or stored on information systems in an unprotected form. User IDs and passwords must not be hard coded in scripts or clear text files such as system shell scripts and batch jobs.

6.2q All users must sign a statement agreeing to keep their personal passwords confidential and to limit group passwords to only members of the group.

Compliance

Group Information Security will regularly assess for compliance against this policy. Any violation of this policy will be investigated and if the cause is found due to wilful disregard or negligence, it will be treated as a disciplinary offence. All disciplinary proceedings are coordinated through the Human Resources Department.

The Royal Mail Group reserves the right to amend this policy at any time and will publish updated versions to all staff.

Associated policies, guidelines and procedures

Policy Statement Ref.	Title of policy, guidelines or procedure
6.2m , 6.2n	*Guidelines for User Access Management*

ISO 27002 controls addressed

A8.3.3, A11.2.1, A11.2.2, A11.2.3, A11.2.4, A11.3.1, A11.5.2, A11.4.1, A11.6.1

4) Access Control Policy

Purpose of the policy

To ensure that the access control requirements to the Royal Mail Group information and information systems are appropriately defined.

Risks and implications

A failure to comply with this policy could expose the Royal Mail Group to accidental or deliberate misuse of information systems, breaches of confidentiality, malicious or accidental corruption of data, theft of intellectual property and a breach of our legislative, regulatory and/or contractual requirements, including the Data Protection Act (1998) and PCI DSS.

Who does this policy apply to?

All Royal Mail Group employees and all agents, contractors, consultants and business partners (hereafter referred to as 'users') requiring business access to the Royal Mail Group information and information systems.

Scope of the policy

All information and information systems developed by or on behalf of Royal Mail Group, including joint venture companies and outsourced units.

RMG00000318

Policy statements

It is the policy of the Royal Mail Group that:

6.2r Appropriate physical and logical access controls, in line with the business, security, legislative and regulatory requirements and as determined by a risk assessment, must be established and documented for all Royal Mail Group information and information systems.

6.2s Information systems processing or storing strictly confidential information must be segregated from other information systems. The requirements and controls for the additional segregation of networks and information systems must be determined following a risk assessment.

6.2t All access originating from untrusted networks (e.g. the Internet) into the Royal Mail Group network and all internal access to information systems processing or storing information classified as strictly confidential must use an approved two-factor authentication mechanism.

6.2u All third-party access to the Royal Mail Group network and information systems must adhere to the same access restrictions as internal users in accordance with the *Third-Party Access Policy*.

6.2v All critical information systems and applications must limit and enforce access times. The operating times for both batch jobs and interactive sessions must be limited to only the times identified as necessary for completion of Royal Mail Group business processes. All access to these systems and applications at all other times must be disabled or suspended.

6.2w All user, system and application sessions that are inactive for a pre-determined amount of time must be automatically terminated. The amount of time permitted before session termination must be aligned with the criticality of the information. Approved compensating controls, e.g. password protected screensavers or terminal locks, must be activated for information systems and applications that cannot automatically terminate sessions.

6.2x All critical information systems and applications must not allow users to have multiple concurrent sessions on the same system.

6.2y All information systems must have, or support, password management systems that are interactive and can ensure strong passwords to meet the requirements of the *User Access Management Policy*.

6.2z All information systems must not transmit passwords in clear text and passwords must not be visibly displayed on the system when being entered.

6.2aa Users given the opportunity to login to information systems must be presented with a login banner. This must include a special notice which informs the user that the system is to be used only by authorised users and that the use of this system constitutes consent to monitoring. Any additional information that identifies the Royal Mail Group, network, location or host name must not appear.

6.2bb All information systems, databases and applications that store user ID and password information must be encrypted with access restricted to only authorised personnel.

6.2cc Utilities that are capable of overriding information system and application controls or performing low-level system maintenance must be approved with additional controls implemented in order to restrict their use.

Compliance

Group Information Security will regularly assess for compliance against this policy. Any violation of this policy will be investigated and if the cause is found due to wilful disregard or negligence, it will be treated as a disciplinary offence. All disciplinary proceedings are coordinated through the Human Resources Department.

The Royal Mail Group reserves the right to amend this policy at any time and will publish updated versions to all staff.

Associated policies, guidelines and procedures

Policy Statement Ref.	Title of policy, guidelines or procedure
6.1d	*Third-Party Access Policy*
6.1h	*User Access Management Policy*

RMG00000318

ISO 27002 controls addressed

A.11.1, A.11.5, A.11.6