YOUR IM

information integration innovation

Date: 5 July 2010

Transport for London

Code of Connection Policy Version 1.3
Partner Edition

Status	Final
Version	1.3
Review	31 May 2011

Table of Contents

Status	Final
Version	1.3

1. Code of Connection Policy

TfL Code of Connection Policy Version 1.3

PARTNER EDITION

Third party partner organisations that require connectivity to Transport for London's, and/or its' group companies' or any of their associated operating company's ("TfL", "TfL's" "we", "us" or "our"), data network(s), to provide or receive services must abide by the terms and conditions described below (the Code of Connection policy, "CoCo policy"). Read only access to our public web servers from the Internet is not subject to the terms of this CoCo policy.

This CoCo policy serves to protect both TfL's and your organisation's interests by providing specific terms and conditions in relation to the use of TfL's applications, IT systems and IT infrastructure (all together and any part of them being the "IT") which you and your organisation agree to abide by. It is a condition of TfL permitting access to the IT that your organisation complies at all times with this CoCo policy.

Failure to comply with any of the terms of this CoCo policy shall permit TfL to suspend or terminate (either immediately or on notice at its option) your and your organisation's use of one or more of our IT including but not limited to applications and/or our file upload or download services at any time. You and your organisation agree to comply with and you agree to procure that all the members of your organisation who have access to any IT in this way, in a business context, comply with the following terms:

1. Any breach, or suspected breach, of security in relation to the use of any of the IT must be reported by you or a member of your organisation to the TfL IM Operations Security Manager at the earliest possible time and definitely within 48 hours of its discovery.
2. All users of TfL's IT must ensure that PCs/terminals that have a logged in session to any IT or service are locked if left unattended for any period of time.
3. Users of TfL's IT must not attempt to circumvent any security controls, determine or identify passwords or breach TfL's access control systems, whether belonging to TfL, its suppliers or other third parties.
4. TfL reserves the right to audit the configuration of any of your IT and systems that are used to connect to any of our IT and you and your organisation give TfL full rights to request such an audit at any time on 5 working days' notice to your organisation. The scope of the audit

Status	Final
Version	1.3
Review	31 May 2011

process is limited to checking compliance with the terms set out in this Agreement. We do not expect you to provide us with direct access to your systems and IT but we do expect you to allow us to audit and/review any and all configuration items that are required for you to comply with the terms of this CoCo policy, such as anti-virus pattern file versions. We would prefer to review these configuration items under the supervision of your staff and you will provide us with such a supervisor on the day or days of audit unless agreed otherwise in writing.

5. Your organisation must refrain from infringing third party copyright, licensing requirements or terms or other intellectual property rights and, without prejudice to the generality of the foregoing, especially those that could impact upon TfL.
6. Virus scanning must be enabled by your organisation on all third party hardware that are used to upload or submit files or access any IT or TfL system.
7. Virus scanning signatures must not be more than 48 hours out of date (in relation to virus definitions released by your organisation's chosen anti-virus vendor(s)) on any system or hardware that is involved in submitting files to any IT or TfL system or storing files on TfL's behalf, including but not limited to, third party systems. Your organisation must use virus scanning software from reputable anti-virus vendor(s) in accordance with industry best practice.
8. Third party users, whether you, your organisation or users within your organisation or otherwise, are not permitted to share their TfL logon credentials, passwords or 2-factor token with any other person. Failure to follow this directive shall permit TfL to invoke removal of access rights for the individual concerned and TfL will notify your organisation's management team of the issue.
9. Third parties, including you and your organisation and your organisation's users, must not upload, to TfL or the IT, any of the file types specified in TfL's Blocked Files Policy (which is incorporated into this Agreement) unless permission to do so is granted in writing by TfL; these are:
    a. EXE, .XPI, .COM, .LNK, .PIF, .SHB, .SYS, .VXD, .HTA, .DLL, .SO, .LIB, .OBJ, .OCX, .VBX, .SCR, .CHM, .SCT, .WSC, .WSF, .WSH, .CPL, .MSC, .REG, .PY, .VBS, .BAT, .CMD, .CSH, .KSH, .SH, .DRV, .MSI
    b. .HLP, .ADE, .ADP, .MDA, .MDB, .MDE, .MDW
    c. .MP2, .MP4, .MP4A, .AAC, .M4A, .M4P, .AC3, .WMA, .WMV, .MPG, .MPEG, .MP3.
10. Devices used to access any of our IT from third party locations must be separated from public networks, such as the Internet, by an adequately secure and technologically advanced firewall. The firewall(s) must be configured in accordance with well known / common best practice guidelines and must have a policy installed that serves to prevent unauthorised access to the third party network.
11. Any third party system or technology that is used to access any of our IT must have adequate security software patches[1] applied in line with vendor recommendations. It is acceptable to use alternative adequate mitigation options if there is an issue with the deployment of a particular patch. As an example, most Host Intrusion Prevention tools can be configured to protect un-patched systems against specific vulnerabilities.

[1] CPNI recommendations for patch management are available from : http://www.cpni.gov.uk/Docs/re-20061024-00719.pdf

12. Your organisation may only connect to the IT for legitimate business purposes and as agreed with TfL.
13. Your organisation is only permitted to upload files that are specifically related to TfL’s business interests.
14. Your organisation must inform their TfL contact within 48 hours when any one of your organisation’s users who has access to any IT no longer requires access to that system.
15. Subject always to paragraph 24 (which takes precedence over this paragraph 15 to the extent of any inconsistency), we reserve the right to monitor and/or record individual use within your organisation of our IT and of ICT facilities for legitimate purposes including without limit to protect against misuse and to ensure system and operational efficiency and integrity and we reserve the right to access individual accounts on our systems and IT in circumstances where we have a reasonable belief that there has been a breach of this CoCo policy.
16. Subject always to paragraph 24 (which takes precedence over this paragraph 16 to the extent of any inconsistency), you must ensure that your organisation (including its users of the IT) must have no expectation of privacy (other than as provided for by law) whilst using our IT. The scope of this paragraph is limited to IT that is managed by TfL or managed on our behalf by a third party.
17. Users of the IT must ensure that they do not download, upload, create or transmit material that is illegal, abusive or threatening to others or might be regarded as offensive on the basis of personal characteristics such as race, sex, colour, religion, nationality, gender, disability, sexual orientation or age.
18. Third party users, whether you, your organisation or otherwise, must not use or attempt to use the IT or attempt to access TfL data that they are not authorised to use or access.
19. Third party users, whether you, your organisation or its users or otherwise must not retain TfL information on any non-TfL equipment unless authorised to do so.
20. TfL reserves the right to terminate or suspend access to the IT (a) immediately at any time if any of the terms in this Coco policy are breached; or (b) at any time if we change the way in which we allow third parties to use our systems and IT; or (c) otherwise on giving notice in writing.
21. Your organisation shall ensure that it issues all users of our IT within your organisation with a copy of our Acceptable Use Policy (“AUP”). Each user must read the AUP before being granted access to our IT. Your organisation shall procure that each user complies with the AUP. Any breach by a user of the AUP shall be deemed to be a breach of the organisation and of this CoCo policy.
22. Your organisation must not use or attempt to use the IT or attempt to access any TfL data that your organisation is not authorised to use or access.
23. Your organisation must not keep TfL’s information or data for any longer than is necessary to complete any work that TfL has agreed your organisation needs the information or data for.
24. TfL shall only exercise any and all of its rights under this Agreement in accordance with and as permitted by law including without limit the Human Rights Act 1998, the Data Protection Act 1998, and the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000.
25. In this CoCo policy, a reference to your organisation includes the organisation and all of its employees, directors and officers as well as your organisation’s individual contractors and

subcontractors (but only if TfL has agreed in writing they can also work with TfL as part of your organisation).

26. In this CoCo policy, a reference to TfL means TfL and all members of the TfL Group (whether subsidiary companies or otherwise) and all of its associated operating companies, including without limit Surface Transport, London Underground and London Rail.

2. This part to be issued to applicable 3rd Party End Users

Third Party User Acceptable Use Policy

PARTNER EDITION

You are required to read and abide by the terms and conditions described below. These terms and conditions are known as the Acceptable Use Policy (“AUP”). The AUP relates to the use of any of Transport for London’s and/or its’ group companies’ or any of their associated operating company’s (being referred to in this AUP as “TfL”, “TfL’s” “we”, “us” or “our”) applications, IT systems and IT infrastructure (one, more or all of any applications, IT systems and IT infrastructure being referred to in this AUP as the “IT”). .

If you are a user of any TfL’s IT then you must read this AUP. If you have any concerns, or do not understand the AUP or your obligations under it, then you must discuss these with your line manager within the organisation for which you work (which we refer to below as the “organisation”). Your line manager can arrange for this AUP to be discussed with you in confidence. In consideration of the work that TfL and your organisation are doing together you are agreeing yourself to comply at all times with the terms and conditions set out below in this AUP. It is a condition of TfL permitting access to any of the IT that you comply at all times with this AUP.

Failure by you to comply with any of the terms of this AUP shall permit TfL to suspend or terminate your use of the IT and/or the file upload or download service at any time. You agree to comply with the terms above and with the following terms:

1. Any breach, or suspected breach, of security in relation to the use of any of the IT must be reported by you or a member of your organisation to the TfL IM Operations Security Manager at the earliest possible time and definitely within 48 hours of its discovery.
2. You must ensure that PCs/terminals that you are using that have a logged in session to any IT or service are locked if left unattended for any period of time.
3. You must not attempt to circumvent any of our security controls, determine or identify passwords (unless authorised by TfL to do so) or breach TfL’s access control systems, whether belonging to TfL, its suppliers or other third parties.
4. You must make sure that the files and data that you upload to our IT do not infringe third party copyright or licensing agreements or other intellectual property rights of TfL or of a third party.

5. You must not share your logon credentials, passwords, 2-factor token or your 2-factor token PIN number with any other person and failure to do so shall permit TfL to remove your access rights and we may choose to notify your organisation's management team of the issue.
6. You must not upload, to the IT, any of the file types specified in TfL's Blocked Files Policy, unless permission to do so is granted in writing by TfL, these are:
    a. EXE, .XPI, .COM, .LNK, .PIF, .SHB, .SYS, .VXD, .HTA, .DLL, .SO, .LIB, .OBJ, .OCX, .VBX, .SCR, .CHM, .SCT, .WSC, .WSF, .WSH, .CPL, .MSC, .REG, .PY, .VBS, .BAT, .CMD, .CSH, .KSH, .SH, .DRV, .MSI
    b. .HLP, .ADE, .ADP, .MDA, .MDB, .MDE, .MDW
    c. .MP2, .MP4, .MP4A, .AAC, .M4A, .M4P, .AC3, .WMA, .WMV, .MPG, .MPEG, .MP3.
7. You may only connect to the IT for legitimate business purposes and as agreed with TfL.
8. You are only permitted to upload files that are specifically related to TfL's business interests.
9. We reserve the right to monitor and/or record your use of our IT and ICT facilities for legitimate purposes to protect against misuse and to ensure system and operational efficiency and integrity. We reserve the right to access individual accounts on our systems and IT in circumstances where we have a reasonable belief that there has been a breach of this AUP. We shall only exercise our rights under this paragraph in compliance with law.
10. Users of TfL systems and applications must have no expectation of privacy whilst using our ICT facilities. The scope of this clause is limited to systems and applications that are managed by TfL or managed on our behalf by a third party. We shall only exercise our rights under this paragraph in compliance with law and your statutory rights are not affected, including any rights you may have under the Human Rights Act 1998, the Data Protection Act 1998 or otherwise.
11. You must not upload, download, create or transmit material that is illegal, abusive or threatening to others or might be regarded as offensive on the basis of personal characteristics such as race, sex, colour, religion, nationality, gender, disability, sexual orientation or age on, from or using any of our IT.
12. You must not use or attempt to use IT or attempt to access TfL's data that you are not authorised to use or access.
13. You must not keep TfL's information or data for any longer than is necessary to complete any work that TfL has agreed you or your organisation need the information or data for. If you are in any doubt then ask your manager for advice.
14. You must not keep TfL's information or data on any non-TfL equipment unless authorised by TfL to do so.

Your organisation has agreed to be bound by this Acceptable Use Policy.

The terms of this AUP are governed by English law and are subject to the English Courts.

Status	Final
Version	1.3