Agreement for the Provision of KCOM PIA

Schedule 8: Security

1. Introduction

1.1 The CP shall ensure that it and all CP Personnel comply with KCOM's security requirements set out in this Schedule which sets out various practical security procedures and the KCOM Security Policy.

1.2 The CP's compliance with KCOM's security requirements and policies set out in this Schedule will be subject to reasonable KCOM audit and independent third-party audits.

2. CP's Obligations

2.1 The CP, its subcontractors and CP Personnel shall be authorised to access KCOM Systems and KCOM Information in accordance with the provisions of this Schedule 8 or Schedule 2 as applicable.

2.2 The CP shall identify to KCOM details of the CP Security Contact - a single point of contact for any security issues such as a senior manager or chief information officer responsible for security and a CP Security Contact available on a 24/7 basis for any urgent security issues as further described in clause 17.3(a).

2.3 The CP Security Contact shall at all times ensure that only CP Personnel who have a need to access, strictly on a "need to know" basis in order to order and receive Physical Infrastructure Access services, are authorised.

3. Access to KCOM Systems

3.1 Any CP and CP Personnel access that KCOM may allow will be solely for the purpose of enabling the CP to order and receive Physical Infrastructure Access services under this Agreement.

3.2 In relation to access to the KCOM System, the CP shall ensure that:

(a) all CP Personnel have unique user IDs and security credentials and never share these user IDs, security credentials etc;

(b) physical access to computer equipment having access to KCOM Systems or storing KCOM Information obtained using access is security credentials-protected; and

(c) the CP conducts regular internal audits to ensure compliance with these provisions.

In the event of any inconsistency between the provisions of clause 3.2 above and the KCOM

Security Policy, the KCOM Security Policy shall prevail.

3.3 The CP and CP Personnel shall access any KCOM supplied access to the internet/intranet appropriately (to enable the CP or CP Personnel to provide the Services).

3.4 In relation to interconnection with KCOM Systems and access to KCOM Information, the CP shall (and, where relevant, shall procure that all CP Personnel shall):

(a) ensure each individual user has a unique user identification and security credentials known only to such user;

(b) ensure each individual receives appropriate security training in the use, handling and management of security credentials and information;

(c) promptly provide to KCOM such reports as KCOM shall from time to time reasonably require concerning the CP's access, use and security of interconnection with KCOM Systems and access to KCOM Information and any related matters;

(d) ensure that physical access to computer equipment having interconnection with KCOM Systems and access to KCOM Information or storing is protected with security credentials to reflect the CP's obligations under this Agreement;

(e) ensure that no onward bridging or linking to KCOM Information of KCOM Systems is permitted;

(f) use reasonable endeavours to ensure no Viruses or malicious code (as the expression is generally understood in the computing industry) are introduced via access to and that there is no corruption of KCOM Systems and/or KCOM Information;

(g) not have or permit interconnection with KCOM Systems and access to KCOM Information other than for the proper performance by the CP of its obligations under and in accordance with this Agreement;

(h) take all reasonable steps to prevent unauthorised interconnection with KCOM Systems and access to KCOM Information;

(i) notify the KCOM Security Contact of any changes to its access method, including the provision of network address translation;

(j) ensure that any KCOM Information is protected by a currently non deprecated National Cyber Security Centre (NCSC) approved level of encryption when transmitted over a non KCOM network; and

(k) notify KCOM promptly should any CP Personnel no longer require access to the KCOM Systems or KCOM Information, thus enabling KCOM to disable the access rights to systems and information.

3.5 If access by CP Personnel to KCOM Information is via CP Systems, or KCOM Systems the CP shall comply with the following provisions:

(a) ensure each individual has a unique user identification and security credentials known only to such CP Personnel for their sole use;

(b) allow access to KCOM 's Information to the minimum required to enable the CP Personnel to perform their duties in connection with this Agreement;

(c) allow access to CP Personnel holding or accessing KCOM's Information using a secure login process;

(d) ensure that the allocation and use of enhanced privileges and access to sensitive tools and facilities in CP Systems are controlled and limited to only those users who have a legitimate business need;

(e) provide processes to ensure that remote and home working activities are subject to appropriate security controls within the CP's organisation including but not limited to remote access by users being subject to strong authentication;

(f) use reasonable endeavours to ensure that users follow NCSC security best practice in the management of their security credentials;

(g) implement a security credentials management system which provides a secure and effective interactive facility that ensures quality security credentials;

(h) ensure that user sessions are terminated after a defined period of inactivity;

(i) ensure that audit logs are generated to record user activity, security credential allocation and security-relevant events and securely managed and retained with no ability on the part of the CP to allow any unauthorised access or amendment to the audit logs;

(j) ensure that monitoring of audit and event logs and analysis reports for anomalous behaviour and/or attempted unauthorised access are performed by CP Personnel independent of those users being monitored;

(k) ensure that development, test and live environments are segregated from each other;

(l) implement controls to detect and protect against malicious software and ensure that appropriate user awareness procedures are implemented;

(m) control changes to an individual CP System configuration through formal change control procedures and protect all documentation relating to CP Systems from unauthorised access or amendment;

(n) use reasonable endeavours to (and, where relevant, shall procure that all CP Personnel) ensure no Viruses or malicious code (as the expression is generally understood in the computing industry) are introduced via access to and use of the

KCOM Systems that there is no corruption of KCOM Systems and/or KCOM Information; and

(o) ensure that any software that undermines the security obligations within this Agreement is identified and removed from CP Systems.

3.6 The CP shall use reasonable endeavours to ensure that CP Personnel who hold and use KCOM's Information on personal computers and mobile computing devices are responsible for ensuring that the personal computers and mobile computing devices are reasonably protected from unauthorised access.

3.7 The CP shall encrypt all Confidential Information if stored on a mobile computing device or in the event of any transmission of Confidential Information by CP Personnel outside of the KCOM System. Any Laptops and PCs containing Confidential Information shall have the whole of the disk encrypted. Devices that do not allow whole-disk encryption, such as memory sticks, CD/DVDs and electronic handheld devices, shall be subjected to additional controls such as:

(a) use of file encryption where available; or

(b) use of application security credential facilities; and

(c) where the device is "pocket-sized", it should be kept with the owner at all times or appropriately secured when it is not.

3.8 The CP shall inform the KCOM Security Contact immediately upon its becoming aware of any actual or suspected unauthorised interconnection with KCOM Systems and access to KCOM Information or misuse of KCOM Systems or KCOM Information or breach of any of the CP's obligations under this paragraph 3.

3.9 KCOM Information obtained from KCOM Systems will be deemed confidential information for the purposes of clause 20 of the Agreement and must not be kept, stored, processed or transferred save to the extent necessary for the CP to order and consume the Service.

3.10 The CP may be required to accept from time to time additional terms and conditions relating to KCOM Systems and imposed by KCOM 's third party suppliers. If the CP refuses or fails to accept such terms and conditions then it will no longer be able to access or use the relevant KCOM System.

3.11 KCOM shall use reasonable efforts to provide the CP with advance notice of any planned downtime or outages of KCOM Systems.

4. Access to the CP Systems

4.1 If KCOM has reasonable grounds for an investigation under the terms of this Agreement and can demonstrate such grounds to the CP and if CP Personnel are granted access to CP Systems that hold, process or provide access to KCOM Information, the CP shall:

(a) ensure each of the CP Personnel has a unique user id and security credentials known only to such CP Personnel for his/her sole use; and

(b) promptly provide KCOM with such reports as KCOM shall from time to time reasonably require concerning CP use and security of access to CP Systems.

5. Investigation

5.1 The CP (or its nominated subcontractor) shall fully cooperate with KCOM in relation to any investigation into breaches by the CP (or CP Personnel) of KCOM ’s security provisions as set out in this Schedule 8 and/or the KCOM Security Policy (which KCOM reasonably believes to have taken place and can substantiate such belief by providing evidence to the CP).

5.2 The CP shall promptly report any potential misuse of KCOM Information or improper or unauthorised access to KCOM Systems and KCOM Information that the CP becomes aware of and, at KCOM ’s request, provide to KCOM a written report with details of the potential misuse, and where necessary a remedial plan and a timetable for achievement of the planned improvements and steps to be taken to avoid further potential misuse.

5.3 If any audit or investigation reveals a risk to the confidentiality, integrity or availability of KCOM Information in the CP's processes or systems, the CP shall, at its own cost, promptly remedy any such risk.

5.4 The CP shall cooperate with KCOM during any reasonable investigation into any suspected breach of this Schedule, including providing reasonable access, accommodation, facilities and assistance to all CP Systems as is reasonably necessary. This shall also include permitting KCOM to interview any relevant CP Personnel and providing KCOM with any available evidence it may reasonably require to aid the investigation.

6. KCOM Obligations

6.1 In relation to where the CP interconnects with KCOM Systems to access KCOM Information, KCOM shall (and, where relevant, shall procure that all KCOM personnel shall) use reasonable endeavours to ensure no Viruses or malicious code (as the expression is generally understood in the computing industry) are introduced via access to and use of the KCOM Systems that there is no corruption of CP Systems and/or CP Information.

6.2 If access by KCOM personnel to CP Information is via KCOM Systems, KCOM shall implement controls to detect and protect against malicious Software and shall access CP Information in line with KCOM's normal business practices in relation to the access of third party information.