East Midlands Strategic Commercial Unit

VERSION CONTROL

Version No.	Date	Author	Post	Reason for Issue
V1.0	11th January 2013	Graeme Unwin	Procurement Policy Manager	
V1.1	24th March 2014	Pat Stocker (on behalf of Force ISO's)	ISO	Clarification on Police / Personal data
V1.2	26th June 2014	Michelle Tilston	Solicitor (EMPLS)	Legal review

Data and Systems Handling and Security (Category 2 Suppliers - *who process and store Police data excluding personal data outside Force systems*)

1. **Definitions**

1.1 Where used in this Schedule:

1.1.1 the term **"Force"** means the Derbyshire / Nottinghamshire / Northamptonshire Police Force and includes any other term used therefor elsewhere in the Contract.

1.1.2 the term **"Contractor"** will include the term **"Provider"**, **"Supplier"** or **"Consultant"**, where this term is used elsewhere in the Contract to describe the party contracting with the Force.

1.1.3 the term **"Contract"** will be interchangeable with the term **"Agreement"**, where used elsewhere in the Contract or Agreement and shall be deemed to include all schedules and appendices thereto.

1.2 For the purpose of this Schedule the following expressions will have the meanings ascribed to them:

1.2.1 **"Breach of Security"** means the occurrence of unauthorised access to or unauthorised use of Force Premises, the Sites, the Services, the Contractor System or any ICT or data (including Police Data) used by the Force or the Contractor in connection with the Contract.

1.2.2 **"Business Day"** means any day other than a Saturday or Sunday or a public or bank holiday in England.

1.2.3 **"Change Control Procedure"** means the procedure agreed between the parties for making amendments to the Contract.

1.2.4 **"Commercially Sensitive Information"** means information notified to the Force in writing (prior to the commencement of this Contract) which has been clearly marked as Commercially Sensitive Information comprised of information: (a) which is provided by the Contractor to the Force in confidence for the period set out in that notification; and/or (b) that constitutes a trade secret.

1.2.5 **"Confidential Information"** means all information in respect of the business and activities of a party including, without prejudice to the generality of the foregoing, any ideas; business methods; finance; prices, business, financial, marketing, development or manpower plans; customer (including programme participants) lists or details; computer systems and software; products or services, including but not limited to know-how or other matters connected with the products or services manufactured, marketed, provided or obtained by such party, and information concerning such party's relationships with actual or potential clients, customers or suppliers and the needs and requirements of such party and of such persons and any other information which, if disclosed, will be liable to cause harm to such party or which is of a confidential or proprietary nature (including information imparted orally). This definition does not mean the same as "Confidential" as defined in the Government Protective Marking Scheme (GPMS).

1.2.6 **"Contracting Authority"** means any contracting authority as defined in Regulation 5(2) of the Public Contracts (Works, Services and Supply) (Amendment) Regulations 2000 other than the Force.

1.2.7 **"Contractor Confidential Information"** means Confidential Information proprietary to the Contractor.

1.2.8 **"Contractor Personnel"** means all employees, agents, consultants and contractors of the Contractor and/or of any sub-contractor of the Contractor.

1.2.9 **"Contractor Software"** means software proprietary to the Contractor, including but not limited to software which is or will be used by the Contractor for the purposes of providing the Services.

1.2.10 **"Contractor System"** means any ICT system(s) used and controlled by the Contractor in performing the Services.

1.2.11 **"Crown Body"** means any department, office or agency of the Crown.

1.2.12 **"Environmental Information Regulations"** means the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Crown Body or Regulatory Body in relation to such regulations.

1.2.13 **"FOIA"** means the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Crown Body or Regulatory Body in relation to such legislation.

1.2.14 **"Force BCDR Plan"** means such business continuity and disaster recovery plan of the Force that may be notified to the Contractor from time to time.

1.2.15 **"Force Premises"** means premises owned, controlled or occupied by the Force and made available for use by the Contractor or its sub-contractors for the provision of the Services on the terms set out in the Contract or any separate agreement or licence.

1.2.16 **"Force System"** means any computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by or on behalf of the Force, or any of its employees, agents, consultants and contractors, or the Contractor in connection with the Contract and which is owned by, or licensed by a third party to, the Force, or any of its employees, agents, consultants and contractors, and which interfaces with the Contractor System or is used by, or on behalf of, the Force to receive the Services.

1.2.17 **"Good Industry Practice"** means the exercise by the Contractor of that degree of skill, diligence, prudence, foresight and operating practice which, at the relevant time, would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same or a similar business as the Contractor, seeking in good faith to comply with its contractual and other obligations.

1.2.18 **"ICT"** means information and communications technology.

1.2.19 **"ICT Environment"** means the Force System and the Contractor System.

1.2.20 **"Information"** has the meaning given under section 84 of the Freedom of Information Act 2000.

1.2.21 **"ISO"** means the Force Information Security Officer.

1.2.22 **"Law"** means any applicable law, statute, bye-law, regulation, order, regulatory policy, guidance or industry code, rule of court or directives or requirements of any Regulatory Body, delegated or subordinate legislation or notice of any Regulatory Body.

1.2.23 **"Malicious Software"** means any software program or code intended to destroy, interface with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether introduced wilfully, negligently or without knowledge of its existence.

1.2.24 **"Police Data"** means any data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which:

1.2.24.1 is provided to the Contractor by or on behalf of the Force in connection with the Contract,

1.2.24.2 the Contractor is required to generate, process, store or transmit pursuant to the Contract.

1.2.25 **"Regulatory Bodies"** means those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in the Contract or any other affairs of the Force and **"Regulatory Body"** shall be construed accordingly.

1.2.26 **"Request for Information"** means a request for information or an apparent request for information under the Code of Practice on Access to Force Information, FOIA or the Environment Information Regulations.

1.2.27 **"Requirement"** means any requirement, specification or similar document provided by the Force, or forming part of the Contract, which sets out details of the Services.

1.2.28 **"Security Policy"** means such security policy of the Force as may be in force from time to time, including without limitation the Force's ICT Acceptable Use Policy.

1.2.29 **"Services"** means the services to be provided by the Contractor to the Force pursuant to the Contract, including without limitation the supply of goods or products to the Force.

1.2.30 **"Sites"** means any premises from which the Services are provided or from which the Contractor manages, organises or otherwise directs the provision or the use of the Services or where any part of the Contractor System is situated or where any physical interface with the Force System takes place.

1.2.31 **"Staff Vetting Procedures"** means those procedures and departmental policies notified to the Contractor from time to time for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures.

1.2.32 **"Standards"** means those British or international standards, the Force internal policies and procedures, Regulatory Body or Crown Body codes of practice and guidance referred to in the Requirement.

1.2.33 **"Third Party Software"** means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services.

2. **Data Handling**

<u>General</u>

2.1 The Contractor warrants, represents and undertakes for the duration of the Contract that:

2.1.1 it will in using any data or systems under or in connection with the Contract comply in all respects with applicable Law and reasonable requirements of the Force (including without limitation ensuring that it uses Third Party Software approved in writing by the Force for protection against Malicious Software and for encrypting Police Data being transmitted over the internet);

2.1.2 all personnel used to provide the Services will be vetted in accordance with the Staff Vetting Procedures;

2.1.3 it has and will continue to hold all regulatory approvals from Regulatory Bodies necessary to perform its obligations under the Contract;

2.1.4 it has and will continue to have all rights in and to the Contractor Software, any Third Party Software and any other software materials made available by it and/or its sub-contractors to the Force necessary to perform its obligations under the Contract; and

2.1.5 in performing its obligations under the Contract, all software used by or on behalf of it will be currently supported versions of that software and perform in all material respects in accordance with its specification.

Police Data

2.2 The Contractor will:

2.2.1 not delete or remove any proprietary notices contained within or relating to Police Data;

2.2.2 not store, copy, disclose, or use Police Data except as necessary for the performance of its obligations under the Contract or as otherwise expressly authorised in writing by the Force;

2.2.3 to the extent that Police Data is held and/or processed by the Contractor, it will provide that Police Data to the Force, or such of its employees, agents, consultants and contractors as the Force shall specify from time to time, as requested in a format specified by the Force (acting reasonably);

2.2.4 be responsible for preserving the integrity, security and confidentiality of Police Data in its possession or control, or which it uses, and preventing corruption, unauthorised disclosure or loss of the same;

2.2.5 ensure the availability of Police Data held and/or processed by the Contractor (in accordance with the requirements of the Force from time to time) to the Force and such of its employees, agents, consultants and contractors as the Force shall specify from time to time;

2.2.6 perform secure back-ups of all Police Data held on its systems and ensure that up-to-date back-ups are stored off-site in accordance with Good Industry Practice, any Force BCDR Plan or the reasonable requirements of the Force. The Contractor will ensure that such back-ups are available and are delivered to the Force and such of its employees, agents, consultants and contractors as the Force shall specify from time to time, at all times upon request and upon termination or expiry of the Contract; and

2.2.7 ensure that any system (including without limitation any personal computer, laptop, server, storage device and removable media) on which it holds Police Data, including but not limited to back-up data, is a secure and encrypted system meeting Good Industry Practice and complying with any

Security Policy and the Standards and, without limiting the generality of the foregoing in any way, that unencrypted removable media is never used to store, transport or Process any Police Data that is Personal Data, Sensitive Personal Data or IL2/PROTECT (and above).

2.3 If Police Data is corrupted, lost or sufficiently degraded as a result of the Contractor's default so as to be unusable, the Force may at its sole discretion:

2.3.1 require the Contractor (at the Contractor's expense) to restore or procure the restoration of such Police Data to the extent and in accordance, where relevant, with the Force BCDR Plan and the Force Incident Management Policy and will do so as soon as practicable but not later than three (3) Business Days after the discovery of the corruption, loss or degradation; and/or

2.3.2 itself restore or procure the restoration of such Police Data, and will be reimbursed by the Contractor any reasonable expenses incurred in doing so.

2.4 If at any time the Contractor suspects or has reason to suspect that Police Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then it will notify the Force immediately and inform the Force of the remedial action it proposes to take.

Contractor System

2.5 The Contractor shall ensure for the duration of the Contract that, in respect of the Contractor System, it:

2.5.1 has appropriate network defence systems enabled;

2.5.2 maintains in place patching and anti-virus policies and that performance against these is measured and monitored to ensure compliance; and

2.5.3 performs a risk assessment and that appropriate, prudent and cost effective risk treatment measures have been applied

in each case in accordance with Good Industry Practice, any Security Policy and the Standards.

3. **Confidentiality**

3.1 Except to the extent set out in this paragraph 3 or where disclosure is expressly permitted elsewhere in the Contract, each party shall:

3.1.1 treat the other party's Confidential Information as confidential in accordance with Good Industry Practice, any Security Policy and the Standards; and

3.1.2 not disclose the other party's Confidential Information to any other person without the other party's prior written consent.

3.2 Paragraph 3.1 will not apply to the extent that:

3.2.1 such disclosure is a requirement of Law placed upon the party making the disclosure, including without limitation any requirements for disclosure under the FOIA, Code of Practice on Access to Force Information or the Environmental Information Regulations;

3.2.2 such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the other party;

3.2.3 such information was obtained from a third party without obligation of confidentiality;

3.2.4 such information was already in the public domain at the time of disclosure otherwise than by a breach of the Contract; or

3.2.5 it is independently developed without access to the other party's Confidential Information.

3.3 The parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Contract is not Confidential Information. The Force shall be responsible for determining in its absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of the FOIA.

3.4 Notwithstanding any other term of this Contract, the Contractor hereby gives his consent for the Force to publish the Contract in its entirety, including from time to time agreed changes to the Contract, to the general public.

3.5 Subject to paragraph 3.6, the Contractor may only disclose Confidential Information to Contractor Personnel directly involved in the provision of the Services and who need to know the information, and will ensure that such Contractor Personnel are aware of and comply with these obligations as to confidentiality, except that the Contractor shall not disclose any Confidential Information to any sub-contractor without the prior written consent of the Force.

3.6 The Contractor shall not disclose Confidential Information to any sub-contractor without the prior written consent of the Force.

3.7 The Contractor will not, and will procure that the Contractor Personnel do not, use Confidential Information received otherwise than for the purposes of the Contract.

3.8 At the written request of the Force, the Contractor shall procure that those Contractor Personnel identified in the Force's written request sign a confidentiality undertaking (in such form as the Force shall reasonably require) prior to commencing any work in accordance with the Contract, or at such later date as the Force shall specify in its written request.

3.9 Nothing in the Contract will prevent the Force from disclosing Contractor Confidential Information:

3.9.1 to any Crown Body or other Contracting Authority, and all Crown Bodies or Contracting Authorities receiving such Confidential Information will be entitled to further disclose the Confidential Information to other Crown Bodies or other Contracting Authorities on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown Body or any Contracting Authority;

3.9.2 to any consultant, contractor or other person engaged by the Force or any person conducting an Home Office or Cabinet Office review;

3.9.3 for the purpose of the examination and certification of the Force's accounts; or

3.10 The Force will use all reasonable endeavours to ensure that any Regulatory Body, Crown Body, Contracting Authority, employee, third party or sub-contractor to whom Contractor Confidential Information is disclosed pursuant to paragraph 3.9 is made aware of the Force's obligations of confidentiality.

3.11 Nothing in this paragraph 3 will prevent either party from using any techniques, ideas or know-how gained during the performance of the Contract in the course of its normal business to the extent that this use does not result in a disclosure of the other party's Confidential Information or an infringement of intellectual property rights.

3.12 This paragraph 3 survives termination of the Contract and will continue in full force and effect.

4. **Freedom of Information**

4.1 The Contractor acknowledges that the Force is subject to the requirements of the Code of Practice on Force Information, FOIA and the Environmental Information Regulations and will assist and cooperate with the Force to enable the Force to comply with its Information disclosure obligations.

4.2 The Contractor will and will procure that its sub-contractors will:

4.2.1 transfer to the Force all Requests for Information that it receives as soon as practicable and in any event within two Business Days of receiving a Request for Information;

4.2.2 provide the Force with a copy of all Information in its possession, or power in the form that the Force (acting reasonably) requires within five Business Days (or such other period as the Force may specify) of the Force's request; and

4.2.3 provide all necessary assistance as reasonably requested by the Force to enable the Force to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.

4.3 The Force is responsible for determining in its absolute discretion and notwithstanding any other provision in the Contract or any other agreement whether any Commercially Sensitive Information and/or any other Information is exempt from disclosure in accordance with the provisions of the Code of Practice on Force Information, FOIA or the Environmental Information Regulations.

4.4 In no event will the Contractor respond directly to a Request for Information unless expressly authorised to do so by the Force.

4.5 The Contractor acknowledges that (notwithstanding the provisions of paragraph 3) the Force may, acting in accordance with the Department of Constitutional Affairs' Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000, be obliged under the FOIA, or the Environmental Information Regulations to disclose information concerning the Contractor or the Services:

4.5.1 in certain circumstances without consulting the Contractor; or

4.5.2 following consultation with the Contractor and having taken the Contractor's views into account;

provided always that where paragraph 4.5 applies the Force shall, in accordance with any recommendations of the Code referred to above, take reasonable steps, where appropriate, to give the Contractor advanced notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.

4.6 The Contractor will ensure that all Information is retained for disclosure as required by Law and will permit the Force to inspect such records as requested from time to time.

4.7 This paragraph 4 will survive termination of the Contract and continue in full force and effect.

5. **Security Requirements**

5.1 The Contractor shall comply, and shall procure the compliance of Contractor Personnel, with any Security Policy.

5.2 The Force shall notify the Contractor of any changes or proposed changes to any Security Policy.

5.3 If the Contractor believes that a change or proposed change to any Security Policy will have a material and unavoidable cost implication to the Services it may submit a change request. In doing so, the Contractor must support its request by providing evidence of the cause of any increased costs and the steps that it has taken or will take to mitigate those costs. Any change request shall then be dealt with in accordance with the Change Control Procedure.

5.4 Until and/or unless a change to the fees is agreed by the Force pursuant to paragraph 5.3 the Contractor shall continue to perform the Services in accordance with its existing obligations under the Contract.

6. **Malicious Software**

6.1 The Contractor shall, as an enduring obligation throughout the term of the Contract, use the latest versions of anti-virus definitions available to check for and delete Malicious Software from the ICT Environment.

6.2 Notwithstanding paragraph6.1, if Malicious Software is found, the parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Police Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency.

6.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of paragraph 6.2 shall be borne by the parties as follows:

6.3.1 by the Contractor where the Malicious Software originates from the Contractor Software, Third Party Software or Police Data whilst under the control of the Contractor or Contractor Personnel; and

6.3.2 by the Force if the Malicious Software originates from Force Software or Police Data whilst under the control of the Force or any of its employees, agents, consultants and contractors.

7. **Staffing Security**

7.1 The Contractor shall comply with the Staff Vetting Procedures in respect of all Contractor Personnel employed or engaged in the provision of the Services. The Contractor confirms that all Contractor Personnel employed or engaged by the Contractor at the date of the Contract were vetted and recruited on a basis that is equivalent to and no less strict than the Staff Vetting Procedures.

7.2 The Contractor shall provide training on a continuing basis for all Contractor Personnel employed or engaged in the provision of the Services in compliance with the Security Policy.

7.3 The Contractor shall document the security roles and responsibilities related to the Contractor System, Processing of Police Data and performance of the Services and name the Contractor Personnel assigned to such roles and notify the Force of the same (and any amendments thereto) in writing from time to time.

7.4 The Contractor shall ensure that all Contractor Personnel who have unescorted access to Force Premises will comply with all visitor requirements and standard policies, rules and regulations relating to such Force Premises as the Force shall require from time to time.

7.5 The Contractor shall ensure that only authorised Contractor Personnel have physical and logical access to the ICT Environment and further, in respect of Police

Data and the Force System, only such of those Contractor Personnel who need such access for the purposes of performance of the Services.

8. **Principles Of Security**

8.1 The Contractor acknowledges that the Force places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Sites and security for the Contractor System. The Contractor also acknowledges the confidentiality of Police Data.

8.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security in relation to the Contractor System which:

8.2.1 is in accordance with Good Industry Practice and Law;

8.2.2 complies with the Security Policy;

8.2.3 meets any specific security threats to the Contractor System; and

8.2.4 complies with ISO/IEC27002 and ISO/IEC27001, PASF or equivalent standard in accordance with paragraph 10 of this Schedule.

8.3 Without limiting paragraph 8.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Force from time to time):

8.3.1 loss of integrity of Police Data;

8.3.2 loss of confidentiality of Police Data;

8.3.3 unauthorised access to, use of, or interference with Police Data by any person or organisation;

8.3.4 unauthorised access to network elements, buildings, Force Premises, the Sites, and tools used by the Contractor in the provision of the Services;

8.3.5 use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Police Data; and

8.3.6 loss of availability of Police Data due to any failure or compromise of the Services.

9. **Audit**

9.1 Without prejudice to any other right of audit or access granted to the Force pursuant to the Contract, the Force may at any time conduct an audit for the purpose of assessing the Contractor's compliance with its obligations under this Schedule. The Force shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Contractor or delay the provision of the Services. Subject to the Force's obligations of confidentiality, the Contractor shall (and shall procure that the Contractor Personnel shall) on demand provide the Force (and/or its agents or representatives) with all reasonable co-operation and assistance in relation to each audit, including without limitation all information requested by the Force within the permitted scope of the audit, reasonable access to any Sites, access to the Contractor System and access to Contractor Personnel.

9.2 Where any audit performed pursuant to paragraph 9.1 above reveals any actual or potential security failure or weaknesses, or any other breach by the Contractor of its obligations under this Schedule, the Contractor shall promptly notify the Force of the remedial action which the Contractor proposes in order to remedy such breach. Subject to the Force's written approval, the Contractor shall implement such remedial action in accordance with the timetable agreed with the Force or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where

remedial action is to address a non-compliance with obligations under this Schedule, the remedial action shall be at no additional cost to the Force.

10. **Compliance With ISO/IEC 27001**

10.1 The Contractor shall carry out such regular security audits as may be required by the British Standards Institute in order to maintain delivery of the Services in compliance with security aspects of ISO 27001, PASF or equivalent standard and shall promptly provide to the Force any associated security audit reports and shall otherwise notify the Force of the results of such security audits.

10.2 If it is the Force's reasonable opinion that compliance with the principles and practices of ISO 27001, PASF or equivalent standard is not being achieved by the Contractor, then the Force shall notify the Contractor of the same and give the Contractor a reasonable time (having regard to the extent of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO 27001, PASF or equivalent standard. If the Contractor does not become compliant within the required time then the Force has the right to obtain an independent audit against these standards in whole or in part.

10.3 If, as a result of any such independent audit as described in paragraph 10.3 the Contractor is found to be non-compliant with the principles and practices of ISO 27001, PASF or equivalent standard then the Contractor shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Force in obtaining such audit.

11. **Breach Of Security**

11.1 Either party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to, an actual, potential or attempted breach, provided always that the Force shall only be required to notify to the extent that the Breach of Security affects the Services.

11.2 Upon becoming aware of any of the circumstances referred to in paragraph 11.1, the Contractor shall:

11.2.1 immediately take all steps necessary to:

11.2.1.1 remedy such breach or protect the Contractor System against any such potential or attempted breach or threat; and

11.2.1.2 prevent an equivalent breach in the future.

Such steps shall include any action or changes reasonably required by the Force. In the event that such action is taken in response to a breach that is determined by the Force acting reasonably not to be covered by the obligations of the Contractor under the Contract, then the Contractor shall be entitled to refer the matter to the Change Control Procedure.

11.2.2 as soon as reasonably practicable provide to the Force full details (using such reporting mechanism as may be specified by the Force from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

12. **Risk Assessment**

The Contractor shall undertake regular risk assessments in relation to the provision of the Services, availability of the ICT Environment and Police Data and compliance with its obligations under this Schedule, not less than once every six months and in accordance with the Security Policy and shall provide the results of, and any recommendations in relation to, those risk assessments to the Force promptly in writing following each such risk assessment. Such risk assessment shall include the

identification of any threats or risks, how such threats and risks may be mitigated and how the provision of the Services, availability of the ICT Environment and Police Data and compliance with its obligations under this Schedule may be maintained in the event of any such identified threats or risks materialising. The Contractor shall maintain an up-to-date risk register in connection with the foregoing and make the same available to the Force upon request.