DATA HANDLING SCHEDULE

CATEGORY 1 SUPPLIERS

Publication Scheme:	Y
Title and Version:	Data Handling Schedule Category 1 Suppliers v7
Purpose:	Data Handling Schedule for contracts with Category 1 Suppliers –who process and store personal data and Police data outside Force systems and premises
Relevant to:	All Police Staff and suppliers
Summary:	Data Handling Schedule for contracts with Category 1 Suppliers – who process and store personal data and Police data outside Force systems and premises **NB its use should always be approved by the Information Management Team and Information Security Team**
Author:	East Midlands Police Legal Services
Date:	5 May 2021
Review Date	6 April 2022

VERSION CONTROL

Version No.	Date	Author	Post	Reason for Issue
V1.0	11 May 2015	Michelle Tilston	Solicitor (EMPLS)	
V2.0	30 Oct. 17	Michelle Tilston	Solicitor (EMPLS)	Amended to reflect feedback from Leicestershire and Derbyshire information management teams
V3.0	2 March 2018	Michelle Tilston	Solicitor (EMPLS)	Amended to align to Crown Commercial Services PPN 03/17
V4.0	3 April 2018	Michelle Tilston	Solicitor (EMPLS)	Amended to reflect feedback from Leicestershire and Lincolnshire information management teams
V5.0	30 May 2018	Michelle Tilston	Solicitor (EMPLS)	Amended to reflect feedback from Derbyshire information management team
V6.4	3 March 2020	Michelle Tilston	Solicitor (EMPLS)	Updated following annual review and feedback from Regional information management teams

V7.2	5 May 2021	Michelle Tilston	Solicitor (EMPLS)	Updated following annual review and feedback from regional information management teams

Data and Systems Handling and Security (Category 1 Suppliers- *who process and store personal data and police data outside Force systems and premises*)

1. **Definitions and Interpretation**

1.1 Where used in this Schedule:

1.1.1 the term **"Force"** means [Derbyshire Constabulary][Leicestershire Police][Lincolnshire Police][Northamptonshire Police][Nottinghamshire Police] and includes the Police[,Fire] and Crime Commissioner for [Derbyshire][Leicestershire][Lincolnshire][Northamptonshire][Nottinghamshire] [and] [the Chief Constable of [Derbyshire Constabulary][Leicestershire Police][Lincolnshire Police][Northamptonshire Police][Nottinghamshire Police]];

1.1.2 the term **"Contractor"** shall include the term "**Provider"**, **"Supplier**" or **"Consultant",** where this term is used elsewhere in the Contract to describe the Party contracting with the Force; and

1.1.3 the term **"Contract"** means the agreement between the Force and the Contractor of which this Schedule forms part.

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

1.2.1 **"Breach of Security"** means the occurrence of unlawful or unauthorised access to or unauthorised use of Force Premises, the Sites, the Services, the ICT Environment or any ICT or data (including Police Data) used by the Force or the Contractor in connection with the Contract (and includes a Data Loss Event);

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 the Contract) which has been clearly marked as Commercially Sensitive Information comprised of information which:

1.2.4.1 was provided by the Contractor to the Force in confidence for the period set out in that notification; and/or

1.2.4.2 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, shall be liable to cause harm to such Party or which is of a confidential or proprietary nature (including information imparted orally);

1.2.6 **"Contracting Authority"** means any contracting authority (as defined in Regulation 2(1) of the Public Contracts Regulations 2015) other than the

Force;

1.2.7 **"Contractor BCDR Plan"** shall have the meaning set out in paragraph 13.1;

1.2.8 **"Contractor Confidential Information"** means Confidential Information proprietary to the Contractor;

1.2.9 **"Contractor Personnel"** means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any sub-contractor of the Contractor engaged in the performance of its obligations under the Contract;

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

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

1.2.12 "Controller", "Data Protection Officer", "Data Subject" "Information Commissioner", "Processor", "Personal Data", "Personal Data Breach", "process" and "processing" shall have the meanings given to those terms by Data Protection Law;

1.2.13 **"Crown Body"** means any department, office or agency of the Crown;

1.2.14 **"Data Loss Event"** means any event that results, or may result, in unauthorised access to Personal Data held by the Contractor in relation to the Contract and/or actual or potential loss and/or destruction and/or disclosure of Personal Data in breach of the Contract, including any Personal Data Breach;

1.2.15 **"Data Protection Law"** means the DPA, the UK GDPR, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable Laws relating to processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner;

1.2.16 **"Data Subject Rights Request"** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to Data Protection Law to access, rectify, restrict, erase, enquire or complain about the use of their Personal Data;

1.2.17 **"Dispute Resolution Procedure"** means the dispute resolution procedure set out in the Contract for the resolution of disputes between the Parties;

1.2.18 **"DPA"** means the Data Protection Act 2018;

1.2.19 **"EIR"** 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;

1.2.20 **"FOIA"** means the Freedom of Information Act 2000 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;

1.2.21 **"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;

1.2.22 **"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;

1.2.23 **"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;

1.2.24 **"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 and those Information Security practices as advised by ISO/IEC 27001:2013;

1.2.25 **"ICT"** means information and communications technology;

1.2.26 **"ICT Environment"** means the Force System and the Contractor System;

1.2.27 **"Information"** has the meaning given under section 84 of the FOIA;

1.2.28 **"Law"** means any applicable law, statute, bye-law, regulation, order, delegated or subordinate legislation, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law or directive, notice or requirement of any Regulatory Body;

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

1.2.30 **"PASF"** means the standard set from time to time by the National Policing Information Risk Management Team of the UK Home Office for the storage of and access to Police Data;

1.2.31 **"Police Data"** means any data (including Personal 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:

1.2.31.1 is provided to the Contractor by or on behalf of the Force in connection with the Contract; or

1.2.31.2 the Contractor is required to generate, process, store or transmit for or on behalf of the Force pursuant to the Contract;

1.2.32 **"Protective Measures"** means appropriate technical and organisational measures which may include pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it;

1.2.33 **"Regulatory Body"** means any government department or regulatory, statutory or other entity, committee or body which, whether under statute, rules, regulations, codes of practice or otherwise, is entitled to regulate, investigate or influence the matters dealt with in the Contract or any other affairs of the Force;

1.2.34 **"Request for Information"** means a request for information or an apparent request for information under the Code of Practice on Access to Government

Information, the FOIA or the EIR;

1.2.35 **"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;

1.2.36 **"Security Plan"** means the Contractor's security plan prepared pursuant to paragraph 9;

1.2.37 **"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;

1.2.38 **"Security Tests"** have the meaning set out in paragraph 10.1;

1.2.39 **"Security Policy Framework"** means the Cabinet Office Security Policy Framework;

1.2.40 **"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;

1.2.41 **"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;

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

1.2.43 **"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;

1.2.44 **"Sub-processor"** means any third party appointed to process Personal Data on behalf of the Contractor related to the Contract;

1.2.45 **"Third Party Software"** means software which is proprietary to any third party which is or shall be used by the Contractor for the purposes of providing the Services; and

1.2.46 **"UK GDPR"** has the meaning given in the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

1.3 In this Schedule, a reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended or replaced by any subsequent enactment, modification, order, regulation or instrument.

1.4 Unless the context otherwise requires or set out above, expressions defined in the Contract and used in this Schedule shall have the meaning set out in the Contract.

1.5 Headings are for convenience only and shall not affect the interpretation of this Schedule.

2. Data Handling

General

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

2.1.1 it shall, in accessing or using any data or systems in accordance or in connection with the Contract, comply in all respects with applicable Law and

any 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 Contractor Personnel involved in providing the Services shall be vetted in accordance with the Staff Vetting Procedures;

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

2.1.4 it has and shall 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 shall be currently supported versions of that software and perform in all material respects in accordance with its specification.

2.2 The Force may, at any time on not less than 30 Working Days' notice, revise the provisions of this paragraph 2 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

2.3 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Force may on not less than 30 Working Days' notice to the Contractor amend this Schedule to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Police Data

2.4 The Contractor shall:

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

2.4.2 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;

2.4.3 to the extent that Police Data is held and/or processed by the Contractor, it shall 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);

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

2.4.5 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;

2.4.6 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 shall 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

2.4.7 ensure that any system (including without limitation any paper records, 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 system meeting Good Industry Practice and complying with the 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, Confidential Information or Government Security Classification OFFICIAL (or above).

2.5 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:

2.5.1 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 Security Policy and shall do so promptly and in any event no later than seventy two (72) hours after the discovery of the corruption, loss or degradation; and/or

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

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

Protection of Personal Data

2.7 With respect to the Parties' rights and obligations under the Contract, the Parties acknowledge and agree that:

2.7.1 the Force is the Controller;

2.7.2 the Contractor is a Processor; and

2.7.3 the Contractor may not determine the purposes nor the means of the processing of Personal Data to be undertaken by it under the Contract.

2.8 The Contractor acknowledges that the Force may also engage other Processors to perform services for and on behalf of the Force and the Contractor shall cooperate and interface directly with such third parties as instructed by the Force.

2.9 The Contractor warrants, undertakes and represents that it shall:

2.9.1 (and shall ensure that the Contractor Personnel shall) only use or process the Personal Data for the purpose set out in the Appendix to this Schedule in accordance with instructions from the Force (as set out in the Contract, the Appendix or as otherwise notified in writing by the Force to the Contractor during the term of the Contract) unless it is required to do otherwise by Law. If it is so required, the Contractor shall promptly notify the Force before processing the Personal Data unless prohibited by Law;

2.9.2 without prejudice to paragraph 2.9.1, process the Personal Data only to the extent, and in such manner, as is necessary for the provision of the Services or as is required by Law or any Regulatory Body;

2.9.3 notify the Force immediately if it considers that any of the Force's instructions infringe Data Protection Law;

2.9.4 provide all reasonable assistance to the Force in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Force, include:

2.9.4.1 a systematic description of the envisaged processing operations and the purpose of the processing;

2.9.4.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

2.9.4.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

2.9.4.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data;

2.9.5 have in place appropriate Protective Measures, which have been reviewed and approved by the Force, to protect against a Data Loss Event having taken account of the:

2.9.5.1 nature of the Personal Data which is to be protected;

2.9.5.2 harm which might result from a Data Loss Event;

2.9.5.3 state of technological development; and

2.9.5.4 cost of implementing any measures;

2.9.6 designate a Data Protection Officer if required by Data Protection Law;

2.9.7 ensure that access to Personal Data is limited to those Contractor Personnel who need access to the Personal Data in order to meet the Contractor's obligations under the Contract;

2.9.8 take all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have (or may have) access to the Personal Data and ensure that they are:

2.9.8.1 aware of and comply with the Contractor's duties set out in this paragraph 2.9;

2.9.8.2 subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;

2.9.8.3 informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Force or as otherwise permitted by the Contract;

2.9.8.4 have undergone adequate training in the use, care, protection and handling of Personal Data and are in receipt of specific instructions in respect of the secure handling of confidential and/or sensitive information; and

2.9.8.5 are appropriately technically qualified;

2.9.9 not transfer the Personal Data to any Sub-processor without the prior written consent of the Force;

2.9.10 if the Force consents to the transfer to a Sub-processor, before allowing any Sub-processor to process any Personal Data related to the Contract,

2.9.10.1 enter into a written agreement with the Sub-processor which gives effect to the terms set out in this paragraph 2 such that they apply to the Sub-processor; and

2.9.10.2 provide the Force with such information regarding the Sub-processor as the Force may reasonably require;

2.9.11 without prejudice to paragraphs 2.9.9 and 2.9.10, remain fully liable for all acts or omissions of any Sub-processor;

2.9.12 not transfer or process Personal Data to any country or territory outside the United Kingdom unless the prior written consent of the Force has been

obtained and, if the transfer or process is to be outside the European Economic Area, the following conditions have been fulfilled:

2.9.12.1 the Force or the Contractor has provided appropriate safeguards in relation to the transfer (in accordance with Data Protection Law) as determined by the Force;

2.9.12.2 the Data Subject has enforceable rights and effective legal remedies;

2.9.12.3 the Contractor complies with its obligations under Data Protection Law by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Force in meeting its obligations); and

2.9.12.4 the Contractor complies with any reasonable instructions notified to it in advance by the Force with respect to the processing of the Personal Data; and

2.9.13 at the written direction of the Force, securely destroy or return to the Force the Personal Data (and any copies of it) in accordance with the Appendix to this Schedule unless the Contractor is required by Law to retain the Personal Data.

2.10 Subject to paragraph 2.11, the Contractor shall notify the Data Protection Officer of the Force immediately if it:

2.10.1 receives a Data Subject Rights Request (or purported Data Subject Rights Request);

2.10.2 receives any other communication, complaint or request (including any information notice) relating to either Party's obligations under Data Protection Law; or

2.10.3 receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

2.10.4 becomes aware of a Data Loss Event.

2.11 The Contractor's obligation to notify under paragraph 2.10 shall include the provision of further information to the Force in phases, as details become available.

2.12 Taking into account the nature of the processing, the Contractor shall provide the Force with full assistance in relation to either Party's obligations under Data Protection Law and any complaint, communication or request made under paragraph 2.10 (and insofar as possible within the timescales reasonably required by the Force) including by promptly providing:

2.12.1 the Force with full details and copies of the complaint, communication or request (including any information notice);

2.12.2 such assistance as is reasonably requested by the Force to enable the Force to comply with a Data Subject Rights Request within the relevant timescales set out in Data Protection Law;

2.12.3 the Force, at its request, with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Force);

2.12.4 assistance as requested by the Force following any Data Loss Event;

2.12.5 assistance as requested by the Force with respect to any request from the Information Commissioner's Office or any consultation by the Force with the Information Commissioner's Office;

2.12.6 assistance as requested by the Force in relation to any other complaint or request made; and

2.12.7 the Force with any other information reasonably requested by the Force related to the complaint, communication or request (including any information notice).

2.13 The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this paragraph 2. This requirement does not apply where the Contractor employs fewer than 250 staff, unless the Force determines that the processing:

2.13.1 is not occasional;

2.13.2 includes special categories of data as referred to in Article 9(1) of the UK GDPR and/or Personal Data relating to criminal convictions and offences as referred to in Article 10 of the UK GDPR and clarified by section 10(5) of the DPA; and

2.13.3 is likely to result in a risk to the rights and freedoms of Data Subjects.

2.14 The Contractor shall permit the Force or the Force's representative and/or auditors (subject to reasonable and appropriate confidentiality undertakings) to inspect and audit the Contractor's data processing activities (and/or those of its agents, subsidiaries, Sub-processors and sub-contractors) and comply with all reasonable requests or directions by the Force to enable the Force to verify and/or procure that the Contractor is in full compliance with its data processing obligations under the Contract (including this Schedule).

2.15 The Contractor shall comply at all times with Data Protection Law and shall not perform its obligations under the Contract in such a way as to (or otherwise do or omit to do anything which might) cause the Force to breach any of its applicable obligations under Data Protection Law.

2.16 The Contractor shall, immediately on demand, fully indemnify the Force and keep it fully and effectively indemnified and hold it harmless from and against all costs, claims, demands, expenses (including legal costs and disbursements), losses, actions, damages, proceedings and liabilities of whatsoever nature suffered or incurred by the Force arising directly or indirectly as a result of any breach by the Contractor of its obligations under this paragraph 2.

2.17 The Parties agree that nothing in this Schedule is intended to undermine, exclude or in any way limit the rights of a Data Subject as set out in Data Protection Law.

<u>Contractor System</u>

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

2.18.1 has appropriate network defence systems enabled;

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

2.18.3 has completed and shall comply with the terms of a Code of Connection Agreement which describes the minimum security requirements of the Contractor System;

2.18.4 regularly carries out a risk assessment and that appropriate, prudent and cost effective risk treatment measures have been applied and are in place,

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

3.1.2 not disclose the other Party's Confidential Information to any other person without the other Party's prior written consent; and

3.1.3 not use the other Party's Confidential Information to procure or seek to procure commercial gain or advantage over either the other Party or a third party or to help or assist others to procure a commercial advantage over the other Party or a third party.

3.2 Paragraph 3.1 shall 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 Government Information or the EIR;

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 or EIR, the content of the 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 or EIR.

3.4 Notwithstanding any other term of the Contract, the Contractor hereby gives its 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 shall ensure that such Contractor Personnel are aware of and comply with these obligations as to confidentiality.

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 shall not, and shall 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 Either Party may disclose the other Party's Confidential Information to its legal advisors to the extent necessary for the purpose of providing advice regarding or relating to the Contract and/or the Services.

3.10 Nothing in the Contract shall prevent the Force from disclosing Contractor Confidential Information:

3.10.1 to any Crown Body or other Contracting Authority, and all Crown Bodies or Contracting Authorities receiving such Contractor Confidential Information shall be entitled to further disclose the Contractor 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;

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

3.10.3 for the purpose of the examination and certification of the Force's accounts.

3.11 The Force shall 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 3.10 is made aware of the Force's obligations of confidentiality.

3.12 Nothing in this paragraph 3 shall 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.

3.13 This paragraph 3 shall survive termination of the Contract and shall 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 Government Information, the FOIA and the EIR and shall assist and cooperate with the Force to enable the Force to comply with its Information disclosure obligations.

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

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;

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 EIR; and

4.2.4 not respond directly to a Request for Information unless expressly authorised to do so by the Force.

4.3 Notwithstanding any other provision in the Contract or any other agreement between the Parties, the Contractor acknowledges and agrees that the Force is responsible for determining in its absolute discretion 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 Government Information, the FOIA or the EIR.

4.4 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 ("Code"), be obliged under the FOIA or the EIR to disclose information concerning the Contractor or the Services:

4.4.1 in certain circumstances without consulting the Contractor; or

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

provided always that where paragraph 4.4.1 applies the Force shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate and without putting itself in breach of any applicable Law, to give the Contractor

advanced notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.

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

4.6 This paragraph 4 shall survive termination or expiry of the Contract and shall continue in full force and effect.

5. **Security Requirements**

5.1 The Contractor shall comply, and shall procure the compliance of Contractor Personnel, with the Security Policy and the Security Plan and the Contractor shall ensure that the Security Plan fully complies with the Security Policy and any other reasonable requirements of the Force.

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

5.3 If the Contractor believes that a change or proposed change to the Security Policy shall 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 shall take to mitigate those costs. Any change request shall then be dealt with by the Parties 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 software available to check for and delete Malicious Software from the ICT Environment.

6.2 Notwithstanding paragraph 6.1, if Malicious Software is found, the Parties shall cooperate 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 Good Industry Practice, the Security Policy and the Standards.

7.3 The Contractor shall document the security roles and responsibilities related to the Contractor System, processing of the 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 access to Force Premises shall 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:

7.5.1 only Contractor Personnel authorised by the Force to have physical and/or logical access to the ICT Environment have such access; and

7.5.2 access to the ICT Environment, Police Data and the Force System is limited to those Contractor Personnel who need access for the purposes of performance of the Services and who have completed appropriate system training.

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 of 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 11.

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/or 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. Security Plan

9.1 Introduction

The Contractor shall develop, implement and maintain a Security Plan to apply during the term of the Contract and after the end of such term (as applicable) in accordance with an exit plan which shall be approved by the Force, tested, periodically updated and audited in accordance with this Schedule.

9.2 Development

9.2.1 Within 20 Business Days after the date of the Contract, the Contractor shall prepare and deliver to the Force for approval its full and final Security Plan.

9.2.2 If the Security Plan is approved by the Force, it shall be adopted immediately. If the Security Plan is not approved by the Force, the Contractor shall amend it within 10 Business Days of a notice of non-approval from the Force and re-submit it to the Force for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Business Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Force. If the Force does not approve the Security Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Force pursuant to this paragraph 9.2.2 may be unreasonably withheld or delayed. However, any failure to approve the Security Plan on the grounds that it does not comply with the requirements of this Schedule shall be deemed to be reasonable.

9.3 Content

9.3.1 The Security Plan shall set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:

9.3.1.1 the provisions of this Schedule;

9.3.1.2 the provisions of the Requirement relating to security;

9.3.1.3 ISO/IEC27002 and ISO/IEC27001, PASF or equivalent standard;

9.3.1.4 such data protection compliance guidance as may be produced by the Force;

9.3.1.5 the minimum set of security measures and standards required where the ICT Environment shall be handling Government Security Classification OFFICIAL-SENSITIVE, as determined by the Security Policy Framework;

9.3.1.6 any other extant national information security requirements and guidance, as provided by Information Security Officers; and

9.3.1.7 appropriate ICT standards for technical countermeasures which are included in the Contractor System.

9.3.2 References to standards, guidance and policies set out in paragraph 9.3.1 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

9.3.3 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Contractor shall notify the Force's contract manager of such inconsistency immediately upon becoming aware of the same, and the Force's contract manager shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.

9.3.4 The Security Plan shall be structured in accordance with ISO/IEC27002 and ISO/IEC27001, PASF or equivalent standard cross-referencing if necessary to other Schedules of the Contract which cover specific areas included within that standard.

9.3.5 The Security Plan shall be written in plain English in language which is readily

comprehensible to the staff of the Contractor and the Force engaged in the Services and shall not reference any other documents which are not either in the possession of the Force or otherwise specified in this Schedule.

9.4 Amendment and Revision

9.4.1 The Security Plan shall be fully reviewed and updated by the Contractor annually, or from time to time to reflect:

9.4.1.1 emerging changes in Good Industry Practice;

9.4.1.2 any change or proposed change to the Contractor System, the Services and/or associated processes;

9.4.1.3 any new perceived or changed threats to the Contractor System; and

9.4.1.4 any reasonable request from the Force.

9.4.2 The Contractor shall provide the Force with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Force.

9.4.3 Any change or amendment which the Contractor proposes to make to the Security Plan (as a result of a Force request or change to the Requirement or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Force.

10. **Audit and Testing**

10.1 The Contractor shall conduct tests of the processes and countermeasures contained in the Security Plan ("Security Tests") on an annual basis or as otherwise agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Force.

10.2 The Force shall be entitled to send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Force with the results of such tests (in a form approved by the Force in advance) as soon as practicable after completion of each Security Test.

10.3 Without prejudice to any other right of audit or access granted to the Force pursuant to the Contract, the Force shall be entitled at any time and without giving notice to the Contractor to carry out such tests (including without limitation penetration tests) as it may deem necessary in relation to, and the Contractor's compliance with and implementation of, the Security Plan. The Force may notify the Contractor of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the Services. If such tests impact adversely on the Contractor's ability to deliver the Services in accordance with the Requirement and the Contract, the Contractor shall be granted relief against any resultant under-performance for the period of the Security Tests.

10.4 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 cooperation 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.

10.5 Where any Security Test carried out pursuant to paragraphs 10.2 or 10.3, or audit

performed pursuant to paragraph 10.4, 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 changes to the Security Plan (and the implementation thereof) and/or other remedial action (as applicable) which the Contractor proposes in order to correct such failure or weakness or remedy such breach. Subject to the Force's written approval (in accordance with paragraph 9.4.3 in respect of the Security Plan), the Contractor shall implement such changes or remedial action in accordance with the timetable agreed with the Force or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where a change to the Security Plan or remedial action is to address a non-compliance with the Security Policy or obligations under this Schedule, the change to the Security Plan and/or remedial action (as applicable) shall be at no additional cost to the Force. For the purposes of this paragraph 10, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

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

11.1 The Contractor shall obtain independent certification of the Security Plan or evidence that they are working towards ISO 27001, PASF or an equivalent standard as soon as reasonably practicable and shall maintain such certification for the duration of the Contract.

11.2 If certain parts of the Security Plan do not conform to good industry practice as described in ISO 27002 and, as a result, the Contractor reasonably believes that its certification to ISO 27001 would fail in regard to these parts, the Contractor shall promptly notify the Force of this and the Force in its absolute discretion may waive the requirement for certification in respect of the relevant parts.

11.3 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.

11.4 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.

11.5 If, as a result of any such independent audit as described in paragraph 11.4 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.

12. **Breach Of Security**

12.1 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, or threat to, the Security Plan provided always that the Force shall only be required to notify the Contractor to the extent that the Breach of Security affects the Services.

12.2 Upon becoming aware of any of the circumstances referred to in paragraph 12.1, the Contractor shall:

12.2.1 immediately take all steps necessary to:

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

12.2.1.2 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; and

12.2.2 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.

13. Business Continuity and Disaster Recovery

13.1 Without prejudice to the provisions of paragraphs 2.4.6 and 2.5, the Contractor warrants, represents and undertakes for the duration of the Contract that it shall have an up-to-date business continuity and disaster recovery plan in relation to the performance of the Services, availability of the Contractor System and Police Data and compliance with its obligations under this Schedule sufficient to enable it to maintain or promptly reinstate (within such reasonable time periods as the Force shall from time to time specify) performance of the Services, availability of the Contractor System and Police Data and compliance with its obligations under this Schedule in the event of a disaster or other business interruption ("Contractor BCDR Plan"). The Contractor shall provide the Force with an up-to-date copy of the same whenever requested by the Force and whenever it is amended. The Contractor shall ensure that the Contractor BCDR Plan complements and coordinates with the Force BCDR Plan. The Contractor shall ensure that it is able to implement the Contractor BCDR Plan at any time in accordance with its terms.

13.2 The Contractor shall carry out regular tests (at least once every 12 months) of the Contractor BCDR Plan and shall provide the Force with 6 weeks' prior written notice of such planned test date. The Force shall have the right to observe such tests and the Parties shall meet following such tests to discuss whether any updates or amendments are required to the Contractor BCDR Plan. The Contractor shall provide the Force with full written details of the results of each test.

13.3 The Contractor shall ensure that any tests of the Contractor BCDR Plan do not interrupt or otherwise adversely affect the provision of the Services in accordance with the Contract or the availability of the ICT Environment and Police Data, nor otherwise disrupt the Force's operations.

13.4 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.

Appendix to Data Handling Schedule

Description	Details
Subject matter of the processing	***[to be completed as part of tender process and/or following a DPIA]***
Duration of the processing	***[to be completed as part of tender process and/or following a DPIA – NB it is anticipated that in most cases processing shall cease immediately on termination or expiry of the Contract]***
Purpose of the processing	***[to be completed as part of tender process and/or following a DPIA]***
Lawful basis/es for the processing	***[to be completed as part of tender process and/or following a DPIA]***
Nature of the processing	***[to be completed as part of tender process and/or following a DPIA]***
Type of Personal Data being processed	***[to be completed as part of tender process and/or following a DPIA]***
Categories of Data Subject	***[to be completed as part of tender process and/or following a DPIA]***
Arrangements for return and/or destruction of the data once the processing is complete	***[to be completed as part of tender process and/or following a DPIA]***
Protective Measures	***[to be completed as part of tender process and/or following a DPIA]***