

**SCHEDULE 2-1**  
**INTERPRETATIONS**

<b>Acceptance Procedure</b>	means the procedure of that name as specified in Schedule 2.5.
<b>Acceptance Test</b>	means a test to be conducted in accordance of the provisions of Schedule 2.5.
<b>Acceptance Test Criteria</b>	means the test criteria specified in Schedule 2.5.
<b>Acceptance Test Period</b>	means the period during which the Acceptance Procedure shall be performed, pursuant to the provisions of Schedule 2.5.
<b>Additional Clauses</b>	means the additional Clauses specified in Annex A to this Contract that were requested in the Order by the CUSTOMER and that shall apply to this Contract.
<b>Affiliate</b>	means any person, partnership, joint venture, corporation or other form of enterprise, domestic or foreign, including but not limited to subsidiaries, that directly or indirectly are controlled by, or are under common control with the CONTRACTOR or a Parent Company.
<b>Alternative Clauses</b>	means the alternative Clauses specified in Annex A to this Contract that were requested in the Order by the CUSTOMER and that shall apply to this Contract.
<b>Catalogue</b>	means the catalogue of goods and associated services available for Order under the provisions of the Goods and Associated Services Framework Agreement.
<b>Catalogue Entry</b>	means an item of Goods or Services that has been approved by the AUTHORITY and listed in the Catalogue.
<b>Charges</b>	means the rates and charges set out in Schedule 2-3.
<b>Charges Variation Procedure</b>	means the procedure for varying the Charges specified in Schedule 2-3.
<b>Confidential Information</b>	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and suppliers of either party, including Intellectual Property Rights, together with all information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential.

## ICT GOODS AND ASSOCIATED SERVICES

<b>Contract Change Note</b>	means the contract change note specified in Schedule 2-7.
<b>Contract Change Procedure</b>	means the contract change procedure specified in Schedule 2-7 for making changes to this Contract.
<b>Contract Generated Intellectual Property Rights</b>	means any Intellectual Property Rights created by the CONTRACTOR as a result of the performance by the CONTRACTOR of its obligations under this Contract.
<b>Contracting Authority</b>	means a contracting authority as defined in Regulation 5(2) of the Public Contracts Works Services and Supply (Amendment) Regulations 2000.
<b>CONTRACTOR's Software</b>	means any software in which the Intellectual Property Rights are owned by the CONTRACTOR.
<b>Credits</b>	means the credits to the CUSTOMER's account, calculated in accordance with the provisions of Schedule 2-2.
<b>Data Controller</b>	shall have the same meaning as set out in the Data Protection Act 1998
<b>Data Processor</b>	shall have the same meaning as set out in the Data Protection Act 1998
<b>Data Protection Requirements</b>	mean the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to Processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.
<b>Data Subject</b>	shall have the same meaning as set out in the Data Protection Act 1998
<b>Days</b>	means calendar days.
<b>Default</b>	means any breach of the obligations of any party (including but not limited to fundamental breach or breach of a fundamental term) or any default, act, omission, negligence or statement of any party, it's employees, agents or sub-contractors in connection with or in relation to the subject matter of this Contract and in respect of which such party is liable to the other.

## ICT GOODS AND ASSOCIATED SERVICES

<b>Environmental Information Regulations</b>	mean the Environmental Information Regulations 2004 and any guidance and/or codes of practice issued by the Information Commissioner in relation to such regulations.
<b>Framework Agreement</b>	means the agreement between the AUTHORITY and the CONTRACTOR, under which this Contract is entered into by the CUSTOMER and the CONTRACTOR, for the supply of ICT Goods and associated Services.
<b>FOIA</b>	means the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner in relation to such legislation.
<b>Government Procurement Card (GPC)</b>	means the UK Government's VISA purchasing card.
<b>Information</b>	has the meaning given under section 84 of the Freedom of Information Act 2000.
<b>Intellectual Property Rights</b>	means patents, trade marks, service marks, design rights (whether registrable or otherwise), applications for any of the foregoing, copyright, database rights, trade or business names and other similar rights or obligations whether registrable or not in any country (including but not limited to the United Kingdom).
<b>Invoicing Procedure</b>	means the procedure by which the CONTRACTOR invoices the CUSTOMER, as set out in Schedule 2-4.
<b>Law</b>	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.
<b>Liquidated Damages Period</b>	'not used'
<b>Liquidated Damages</b>	'not used'
<b>Mediator</b>	has the meaning ascribed to it in Schedule 2-9.
<b>Model Contract for ICT Goods and associated Services version 6.00</b>	means the model contract of that name published by OGCBuying.solutions on its website
<b>Month</b>	means a calendar month and "Monthly" shall be similarly construed.

## ICT GOODS AND ASSOCIATED SERVICES

<b>Notice of Arbitration</b>	means the formal notice from the CONTRACTOR or the CUSTOMER to the other party referring a dispute to arbitration in accordance with the provisions of Schedule 2-9.
<b>Order</b>	means an order for Goods and associated Services served by the CUSTOMER on the CONTRACTOR.
<b>Ordered Goods</b>	means items selected by the CUSTOMER and included in Schedule 2-2 of this Contract pursuant to an Order.
<b>Ordered Services</b>	means a services selected by a CUSTOMER and included in Schedule 2-2 of this Contract, pursuant to an Order.
<b>Parent Company</b>	means any company which is the ultimate Holding Company of the CONTRACTOR or any other company of which the ultimate Holding Company of the CONTRACTOR is also the ultimate Holding Company and which is either responsible directly or indirectly for the business activities of the CONTRACTOR or which is engaged in the same or similar business to the CONTRACTOR. The term "Holding Company" shall have the meaning ascribed by Section 736 of the Companies Act 1985 or any statutory re-enactment or amendment thereto.
<b>Payment Profile</b>	means the profile of payments to be made by the CUSTOMER to the CONTRACTOR under the terms of this Contract as set out in Schedule 2-4.
<b>Personal Data</b>	shall have the same meaning as set out in the Data Protection Act 1998.
<b>Pre-Existing Intellectual Property Rights</b>	means any Intellectual Property Rights vested in or licensed to the CONTRACTOR or CUSTOMER prior to or independently of the performance by the CONTRACTOR or CUSTOMER of their obligations under this Contract, but excluding Intellectual Property Rights owned by the CONTRACTOR subsisting in the CONTRACTOR's Software.
<b>Private Authority</b>	means a commercial organisation to whom service provision has been outsourced by a Contracting Authority, which assumes the role and responsibilities of the CUSTOMER under a Contract.
<b>Processing</b>	shall have the same meaning as set out in the Data Protection Act 1998.
<b>Quarter</b>	means a three (3) month period beginning on 1 <sup>st</sup> January, 1 <sup>st</sup> April, 1 <sup>st</sup> July or 1 <sup>st</sup> October. The term

## ICT GOODS AND ASSOCIATED SERVICES

	“Quarterly” shall be similarly construed.
<b>Regulatory Bodies</b>	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 this Contract or any other affairs of the CUSTOMER and "Regulatory Body" shall be construed accordingly.
<b>Reports</b>	means reports submitted by the CONTRACTOR to the CUSTOMER as specified in Schedule 2-6.
<b>Requests for Information</b>	means a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations.
<b>Service Commencement Date</b>	means the date of commencement of the provision of the Ordered associated Services by the CONTRACTOR in accordance with the Order.
<b>Service Credits</b>	means the service credits specified in Schedule 2-2 which shall be payable to the CUSTOMER by the CONTRACTOR in the event that the Service Levels are not met in respect of Ordered Goods and Ordered Services.
<b>Service Levels</b>	means the levels of service defined in Schedule 2-2.
<b>Special Terms</b>	means additional Customer specific terms, to which the CONTRACTOR’s agreement is sought by a Customer under the Further Competition Procedure specified in Schedule 5.
<b>Standards and Regulations</b>	means the standards and regulations as set out in Clause 3 with which the CONTRACTOR shall comply in the supply of the Ordered Goods and the provision of the Ordered Services and its responsibilities and obligations hereunder.
<b>Sub-Contractor</b>	means any supplier selected, appointed and managed by the CONTRACTOR in accordance with the provisions of Schedule 2-8, including the Sub-Contractors specified in Schedule 2-8. The terms “Sub-Contract” and “Sub-Contracting” shall be similarly construed.
<b>Term</b>	means the term of this Contract as set out in Clause 10, subject to early termination pursuant to Clause 10.
<b>Termination Events</b>	means each of the events specified in Clause 10.3.
<b>Third Party Software</b>	means any software in which the Intellectual Property

## ICT GOODS AND ASSOCIATED SERVICES

	Rights are owned by a third party.
<b>Working Days</b>	means Monday to Friday inclusive, excluding English public and bank holidays.
<b>Year</b>	means a calendar year.

## ADDITIONAL INTERPRETATIONS

<b>Access Northern Ireland (or Access NI)</b>	means criminality disclosure organisation for Northern Ireland.
<b>Appeal</b>	means the applicant is given the opportunity to appeal against the licensing decision made by SIA.
<b>Appeal Bundle</b>	means the SIA generate a set of documents (in electronic and hard copy) to submit to the appeals process.
<b>Appeal Outcome Report</b>	means a report presenting the results of the appeal. Produced by the appeal court.
<b>Application</b>	means an application for an SIA Licence.
<b>Application Case</b>	means information held about an applicant and their SIA licence application.
<b>Applicant</b>	means person applying for a SIA Licence.
<b>Approved Contractor</b>	means a contractor approved by the CUSTOMER in accordance with the CUSTOMERS approved contractor scheme.
<b>Approved Operational Resources</b>	means the resources required to provide the managed service Solution which includes but not limited to: call centre agent; document handling administrator, back office administrator, security officer, administration, operations manager and team leaders.
<b>Assets</b>	<p>means all assets and rights to enable the CUSTOMER or a successor contractor to own, operate and maintain the Solution and to provide the Order Good and Ordered Services in the Handover Period in accordance with this Contract, including:</p> <ul style="list-style-type: none"> <li>(a) any CONTRACTOR Premises;</li> <li>(b) any Hardware, copies of Software and Materials;</li> <li>(c) any other books and records</li> </ul>

## ICT GOODS AND ASSOCIATED SERVICES

	<p>(including operating and maintenance manuals, health and safety manuals and other know how);</p> <p>(d) any spare parts, tools and other assets (together with any warranties in respect of assets being transferred);</p> <p>(e) any revenues and any other contractual rights; and</p> <p>(f) any Intellectual Property Rights,</p> <p>but excluding any assets and rights of which the CUSTOMER is full legal and beneficial owner;</p>
<b>Authorised SIA Staff</b>	means all staff employed by the CUSTOMER who are given the appropriate permissions to complete a task or activity.
<b>Availability Plan</b>	<p>means this plan is an essential part of service availability management, in essence it should detail:</p> <ul style="list-style-type: none"> <li>• How the supplier is going to meet the required service and systems availability as required by the defined Service Levels in schedule 2-2.</li> <li>• Any planned outage to the service e.g. for general maintenance or to support a major release of service / system components.</li> <li>• It may also define measures for improving service availability where this is or has become an issue.</li> </ul> <p>The plan should communicate to the CUSTOMER how the service availability Service Level will be met on an ongoing basis. It should also include where planned outages so that the CUSTOMER can take necessary measures, this might include preparing external communications and / or making effective use of staff during periods of down time. The plan will change over time and with new service components being released the plan may need to be updated to incorporate a new service, e.g. E-Fill availability.</p>
<b>Awarding Bodies</b>	means a qualifications body that award certificates in security education & competency.

## ICT GOODS AND ASSOCIATED SERVICES

<b>Acquired Rights Directive</b>	means Council Directive 2001/23/EC on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses;
<b>Bank Holiday(s)</b>	means a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in England and Wales.
<b>Breach of Security</b>	the occurrence of unauthorised access to or use of the CUSTOMER Premises, the Ordered Goods and Ordered Services, the CONTRACTORS Solution or any ICT or data (including the CUSTOMER's Data) used by the CUSTOMER or the CONTRACTOR in connection with this Contract.
<b>Business Continuity Plan</b>	has the meaning set out in paragraph 1.2.2 of schedule 2-15 (Disaster Continuity and Disaster Recovery Provisions)
<b>Business Licensing</b>	means the licensing of businesses operating within the Private Security Industry. Initially targeted at Vehicle Immobilisers.
<b>Business Improvement Group (BIG)</b>	means as defined in Schedule 2-2 and terms of reference set out in the Contract Management Strategy.
<b>Case Note</b>	means additional information held within an application case, relating to the applicant or application for a SIA licence.
<b>Company Sponsor</b>	means the business representative who manages the application and payment of SIA licences on behalf of their employees.
<b>Competency</b>	means the level of training required to meet SIA skill standards in the Private Security Industry.
<b>Configuration Item</b>	means component of the Managed Service Solution.
<b>Contact Centre</b>	means the structured telephony environment (including inbound and outbound operations) where Applicants and License Holders interact with the CONTRACTOR through a single point of contact using various channels including telephony, post, email and fax.
<b>Contract Management Strategy</b>	means a strategy to manage the contract as defined in schedule 2-6
<b>Core Hours</b>	Means 8am to 8pm Monday to Friday excluding Bank Holidays
<b>Crime Stoppers</b>	means a charity organisation offering a public help line to receive information from members of the public who have witnessed potentially criminal behaviour.

## ICT GOODS AND ASSOCIATED SERVICES

<b>Criminal Records Bureau</b>	means criminality disclosure organisation for England & Wales.
<b>Criminality</b>	means a person's criminal record.
<b>CUSTOMER DATA</b>	<p>means all forms of data, text, drawings, diagrams, images or sounds, system parameters, indexing data, logs and archives, e-mail messages and user defined macros (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:</p> <ul style="list-style-type: none"> <li>(i) supplied to the CONTRACTOR by or in behalf of the CUSTOMER; and/or</li> <li>(ii) supplied to the CONTRACTOR by or on behalf any CUSTOMER service recipient; and/or</li> <li>(iii) which the CONTRACTOR is required to generate, process, store or transmit pursuant to this Contract; and/or</li> </ul> <p>b) any Personal Data for which the CUSTOMER and/or CUSTOMER service recipient is the Data Controller.</p>
<b>CUSTOMER Furnished Items</b>	means any items issued or otherwise furnished in connection with this Contract by or on behalf of the CUSTOMER.
<b>Defined Issues</b>	means additional information provided with passport data received from IPS, e.g reported lost or stolen, expired, fraudulent.
<b>Disaster</b>	means the occurrence of one or more events which either separately or cumulatively mean that the Ordered Goods and Ordered Services or a material part of it will be unavailable for a period, or which is reasonably anticipated and will mean that the Order Goods and Ordered Services or a material part will be unavailable for that period
<b>Disaster Recovery</b>	means the process of restoration of the Solution by the provision of the Disaster Recovery Services
<b>Disaster Recovery Plan</b>	has the meaning set out in paragraph 1.2.3 of schedule 2-15 (Business Continuity and Disaster Recovery Provisions)
<b>Disaster Recovery Services</b>	means the disaster recovery [and/or business continuity] services (as the context may require) to be provided by the CONTRACTOR pursuant to schedule 2-15 (Disaster Recovery and Business Continuity Provisions)
<b>Disaster Recovery System</b>	means the system identified by the CONTRACTOR in the CONTRACTOR's Solution which shall be used for

## ICT GOODS AND ASSOCIATED SERVICES

	the purpose of delivering the Disaster Recovery Service;
<b>Disclosure Request</b>	means a request for disclosure of a person's criminal record.
<b>Disclosure Return</b>	means a report of a person's criminal record.
<b>Disclosure Scotland</b>	means criminality disclosure organisation for Scotland
<b>Document Authentication Technology</b>	means IT equipment and software to authenticate the validity of identity documentation (Passports, Driving Licences, Birth Certificates etc)
<b>Document Handling Centre</b>	means the centre for receipt, administration and processing of incoming and outbound post and the scanning, indexing and management and processing of application documentation and criminality checks
<b>Eligibility Checks</b>	means checks made to establish a person's identity, qualifications, right to work and criminal record.
<b>Employment Regulations</b>	means the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced from time to time or any other Regulations implementing the Acquired Rights Directive
<b>Existing Contract</b>	means the contract between SECURITY INDUSTRY AUTHORITY - and - BRITISH TELECOMMUNICATIONS plc relating to the provision of Specialist Solution Services dated 20 March 2007. and related order dated 20 <sup>th</sup> March 2007 and any subsequent signed change control notes relating to that contract and order.
<b>Identity Document Exemption</b>	means exemption from provision of certain identity or criminality documentation as agreed with SIA.
<b>Formal Investigation</b>	means the progression of compliance cases to court.
<b>Front Line Staff</b>	means security staff that are public facing.
<b>General Principles</b>	has the meaning set out in paragraph 1.2.1 of schedule 2-15 (Business Continuity and Disaster Recovery Provisions)
<b>Gross Application</b>	means an Application received into the Document Handling Centre.
<b>Group A</b>	means a set of primary identity documents, such as passport, driving licence or firearms certificate.
<b>Handover Period</b>	has the meaning ascribed by Clause 35.7.

## ICT GOODS AND ASSOCIATED SERVICES

<b>Hardware</b>	means computer, telecommunications and network equipment, including any peripherals, but excludes cabling
<b>HMG Security Policy Framework</b>	means a policy document issued on behalf of Her Majesty's Government providing a framework for improving security within government agencies and contractors providing services to government agencies.
<b>HMG Information Security Standard</b>	means a set of standards for ensuring information security within government departments, issued on behalf of Her Majesty's Government.
<b>iBase</b>	means a database solution to capturing, analysing and organising intelligence information received from multiple sources.
<b>Identity Documents</b>	means a set of documents that are required to establish identity (including passport, driving licence, birth certificate etc).
<b>Identity Document Exemption</b>	means in special cases exemption is given to provision of certain identity documents, in agreement with the CUSTOMER.
<b>Identity &amp; Passport Service</b>	means government agency responsible for issuing UK Passports and UK Identity Cards.
<b>Incident</b>	means interruption to service or significant degradation of service, impacting delivery or service levels and availability of the Solution to the CUSTOMER.
<b>Intelligence Information</b>	means Information offered to the CUSTOMER about a security operative or security business that is allegedly engaged in non-compliant activity.
<b>LDN</b>	means Licence Dispensation Notice see definition.
<b>LDRM</b>	means License Decision Ready to be Made
<b>Licence</b>	means Individual or Business Licence issued by the SIA to Security Operatives and Security Operators.
<b>Licence Card</b>	means SIA Licence Card see definition
<b>Licence Condition</b>	means a set of conditions on the Licence Holder when a SIA Licence is issued e.g. notification of changes to criminality, change of address/name etc.
<b>Licensing Decision</b>	means the decision made by the CUSTOMER, either granting a licence, refusing a licence or 'minded to refuse' a licence.

## ICT GOODS AND ASSOCIATED SERVICES

<b>Licence Dispensation Notice</b>	means provision for an employee of an Approved Contractor to work following submission of an application and prior to issuing an SIA Licence. An Approved Contractor is allowed to deploy up to 15% of their front line workforce with LDNs.
<b>Licence Holder</b>	means the person or business issued with an SIA licence.
<b>Licensable Activity</b>	means one of the designated activities within the PSIA that requires compulsory licensing of individuals. Currently: manned guarding (including security guarding, door supervision, close protection, cash and valuables in transit, and public space surveillance using CCTV), key holding and vehicle immobilising.
<b>Manual Payment Transaction</b>	means payment received for a licence application in the form of a cheque, postal order or banker's draft.
<b>Memorandum of Understanding</b>	means an agreement with another public sector third party for the delivery from or delivery to of services connected with the Solution.
<b>Mental Health Issue</b>	means a declaration by the applicant that they have been subject to compulsory detention under the Mental Health Act in the last 5 years.
<b>Minded to Refuse</b>	means the SIA are likely to refuse to grant a licence unless the applicant can provide mitigating information or evidence of a factual error.
<b>Minded to Revoke</b>	means the SIA are likely to revoke a licence unless the Licence Holder can provide mitigating information or evidence of a factual error.
<b>MP</b>	means Member of Parliament
<b>Multiple Application</b>	means the submission of many applications from a single employer, by the company sponsor.
<b>Net Application</b>	means an Application that has passed all the Validation checks and has therefore been progressed for the Eligibility Checks to begin.
<b>New Cabling</b>	means any voice or data cabling (category 5 standard or as otherwise agreed in writing between the parties) which is added or changed as part of moves and changes projects.
<b>Non Core Hours</b>	means hours outside Core Hours
<b>Non-conviction</b>	means information held about an applicant or Licence Holder that may affect a licensing decision and does not

## ICT GOODS AND ASSOCIATED SERVICES

	relate directly to a previous criminal record.
<b>Non-Front Line Staff</b>	means staff employed in a Private Security business who are not public facing.
<b>Overseas Criminality Certificate</b>	means criminality disclosure report from outside the UK. Required from applicants resident outside the UK for more than 6 months in the last 5 years.
<b>Partner Organisation</b>	means an organisation working in partnership with SIA. This includes law enforcement agencies, local authorities, other government departments (e.g. UKBA & IPS), education organisations or similar.
<b>Pre-Appeal</b>	means following the licensing decision, the applicant has 21 days to lodge an appeal. The pre-appeal stage provides the opportunity for the applicant provide mitigation information or evidence of factual error prior to embarking on legal action.
<b>Privacy Impact Assessment</b>	means a process which enables organisations to anticipate and address the likely privacy impacts of new initiatives, foresee problems, and negotiate solutions to ensure data protection compliance.
<b>Problem</b>	means an issue with the solution or service that is not causing an interruption of service but needs to be reported and potentially resolved.
<b>Protectively Marked / Protective Marking</b>	means the appropriate protective marking such as PROTECT, RESTRICTED, CONFIDENTIAL, SECRET AND TOP SECRET as defined in Schedule 2-13.
<b>PSIA</b>	means Private Security Industry Act 2001
<b>Private Security Industry</b>	means umbrella term representing businesses providing security services in the UK. This does not include 'in house' employed security staff.
<b>Public Register of Licence Holders</b>	means a publicly available register of all SIA licence holders.
<b>Records</b>	means all information, text, drawings, diagrams, images or sounds which are embodied in any electronic or tangible medium (except any Specially Written Software), and which are supplied or in respect of which access is granted to the CONTRACTOR by the CUSTOMER under this Contract, or which the CONTRACTOR is required to generate under this Contract;
<b>Reinstatement</b>	means a licence previously revoked is reinstated.

## ICT GOODS AND ASSOCIATED SERVICES

<b>Rejection Rate</b>	means the percentage of Gross Applications that fail Validation or payment activities and therefore do not progress to the Eligibility Checks.
<b>Related Service Provider</b>	means any person who provides services to the CUSTOMER in relation to the Project from time to time which persons include without limit as at the Effective Date
<b>Release Management</b>	means the managed implementation of changes to IT services taking a holistic (people, process, technology) view which considers all aspects of a change including planning, designing, building, testing, training, communications and deployment activities.
<b>Repeat Incidents</b>	means a persistent failure of any managed element within the Solution the measurement of which is defined in Schedule 2-2 paragraph 3.8.2.1.
<b>Re-submission</b>	means an application is resubmitted to SIA following rejection (application was received incomplete or incorrect).
<b>Revocation</b>	means a licence is removed from a Licence Holder while non-compliant activity or misconduct is investigated.
<b>Right to Work</b>	means establishing whether an applicant not born within the EEA (including Hungary & Romania) has the right to work within the UK. The Right to Work checks are completed in conjunction with UK Borders Authority.
<b>Risk Score</b>	means a rating established for each applicant based on a number of characteristics of their application and previous licence history.
<b>SCRO</b>	Scottish Criminal Records Office also known as “Disclosure Scotland”.
<b>Secondary Licence</b>	means an application for an additional SIA licence within a separate licensable activity.
<b>Security Aspects Letter</b>	means the letter issued in compliance with Cabinet Office best practice guidance which establishes the security provisions with which the CONTRACTOR shall comply in providing the Solution, Ordered Goods and Ordered Services, as such provisions are relevant to the design, development and system administration of the Solution offered under this Contract. The contents of the Security Aspects Letter should be read in conjunction with the detailed security requirements set out in schedule 2.10 (Standards), schedule 2.13 (Security) and the CUSTOMER Requirements in

## ICT GOODS AND ASSOCIATED SERVICES

	respect of security as set out in Schedule 2.2.
<b>Security Incident</b>	means an incident involving a compromise of the Managed Service Solution security measures.
<b>Security Operative</b>	means a person employed in the Private Security Industry.
<b>Security Operator</b>	means a business employing security operatives.
<b>Security Plan</b>	means the CONTRACTOR's security plan prepared pursuant to paragraph 3 of Schedule 2.13 (Security Requirements and Plan);
<b>Security Policy</b>	means the CUSTOMER's security policy as updated from time to time available from the CUSTOMER's security unit;
<b>Security Requirements</b>	as set out Schedule 2-13
<b>Security Tests</b>	means shall have the meaning set out in paragraph 4 of Schedule 2.13 (Security Requirements and Plan);
<b>Service Desk</b>	means the central point of contact for the CONTRACTOR and CUSTOMER on a day to day basis as the focal point for reporting incidents (disruptions or potential disruptions in service availability or quality and service related administration task).
<b>Service Period</b>	means a calendar month during this Contract save that the final payment month of the Contract shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term. The first Service Period of the Contract shall begin on the Service Commencement Date and shall expire at the end of the calendar month in which the Service Commencement Date falls;
<b>Service Transfer</b>	means any transfer of the Ordered Goods and Ordered Services (or any part of the Ordered Goods and Ordered Services), for whatever reason, from the CONTRACTOR or any Sub-Contractor to the CUSTOMER or to a replacement service provider.
<b>Service Transfer Plan</b>	means the plan produced by the CONTRACTOR to be agreed by the CUSTOMER to facilitate any transfer of the Ordered Goods and Ordered Services (or any part of the Ordered Goods and Ordered Services), for whatever reason, from the CONTRACTOR or any Sub-Contractor to the CUSTOMER or to a replacement service provider.

## ICT GOODS AND ASSOCIATED SERVICES

<b>Service Transfer Date</b>	means the date of a Service Transfer.
<b>Shared Use Assets</b>	means those assets which are used by the CONTRACTOR both in connection with this Agreement and for other purposes (which, for the avoidance of doubt, include the provision of a service to a third party and the use of the Asset by the CONTRACTOR for its own legitimate business purposes);
<b>SIA</b>	means Security Industry Authority
<b>SIA HQ</b>	means Security Industry Authority Head Office
<b>SIA Compensation Policy</b>	means a policy designed to compensate applicants or licence holders who have a grievance against the SIA.
<b>SIA Competency Rules</b>	means the rules associated with establishing a level of competency required to operate within a licensable activity.
<b>SIA Compliance &amp; Investigation Team</b>	means SIA team responsible for reducing non-compliance with the Private Security Industry Act.
<b>SIA Guidance Notes</b>	means a document designed to assist the applicant in completing the SIA application form.
<b>SIA Information Communication Technology Team</b>	means internal SIA team responsible for providing IT services to the CUSTOMER. They manage the SIA technical infrastructure and provide first line support to technical issues within CUSTOMER offices and for remote workers.
<b>SIA Intelligence</b>	means SIA team responsible for receiving, analysing and disseminating intelligence information.
<b>SIA Licence Card</b>	means a token representing the granting of a licence to an individual working within the Private Security Industry.
<b>SIA Licensing Criteria</b>	means the criteria to be met by security operatives who wish to work in the private security industry (details provided in the "Get Licensed" publication).
<b>SIA Licensing Operations</b>	means SIA's Licensing Team, responsible for the licence decision making and appeals process.
<b>SIA Records Retention Schedule</b>	means a document defining the retention period for data & information held by the SIA.
<b>SIP</b>	means Service Improvement Plan (SIP): as defined in schedule 2-2

## ICT GOODS AND ASSOCIATED SERVICES

<b>Software</b>	means any and all computer programs in both source and object code form, including all modules, routines and sub-routines comprising such programs and all source and other preparatory materials relating to them, including user requirements, functional specifications and programming specifications, ideas, principles, programming languages, algorithms, flow charts, logic, logic diagrams, orthographic representations, file structures, coding sheets, coding and any manuals or other documentation relating to them and computer generated works;
<b>Sole Use Assets</b>	means those Assets which are owned and used by the CONTRACTOR in connection with this Contract and for no other purpose in the Solution.
<b>Solution</b>	means the technology designed, developed and implemented to support the CUSTOMER business requirements. Normally this is expected to be a system or application but the supplier may choose to implement parts of the solution manually. The solution may therefore include the provision of resources to enable a business process to be completed on behalf of CUSTOMER.
<b>Stakeholder</b>	means organisation with an interest in the SIA.
<b>Sub-Contract</b>	<p>means any agreement between the CONTRACTOR and any third party (including but not limited to the Sub-Contractors listed in Schedule 2-8) for the provision of:</p> <ul style="list-style-type: none"> <li>(a) any of the Ordered Services;</li> <li>(b) facilities or services related to the provision of the Ordered Services other than those which are required to be provided by the CUSTOMER; or</li> <li>(c) facilities or services related to the CONTRACTOR's management, direction or control of the Ordered Services,</li> </ul> <p>and the terms Sub-Contractor and Sub-Contracting shall be similarly construed;</p>
<b>Supporting Evidence</b>	means documentation that supports an applicant's eligibility, including identity documents (passport, birth certificate, evidence of address etc).
<b>Suspension</b>	means the removal of a licence, due to misconduct.
<b>Third Party Software</b>	means any Software employed in the provision of the Ordered Services in which the Intellectual Property Rights are owned by a third party;

## ICT GOODS AND ASSOCIATED SERVICES

<b>TUPE</b>	means Transfer of Undertakings (Protection of Employment) Regulations
<b>Toolset</b>	means any commercially available software that is used in support of a User's work, but which does not in itself constitute an application forming part of the Ordered Services (database packages, spreadsheets, statistical analysis tools and drawing or DTP tools are all examples of Toolsets);
<b>Top Up Certificate</b>	means an additional qualification required to continue working within a given licensable activity.
<b>UK Border Agency</b>	means government agency responsible for immigration and protection of UK borders. UKBA complete Right to Work checks on SIA applicants who were born outside the EEA.
<b>Validation</b>	means the action of checking an Application in accordance with predefined rules and requirements to determine if it is acceptable for onward processing. If acceptable the Application is deemed to have passed Validation. If unacceptable the Application has deemed to have failed Validation.
<b>Validation Status</b>	A stage in the Application process which signifies that the Application and associated documents have been scanned into the core system and the case is ready to be validated via the process known as Validation.
<b>Virtual Library</b>	means an online secure repository where required collections of documents and registers applicable to this Contract are stored in digital formats. The digital content may be stored locally, or accessed remotely via computer networks where security requirements permit.

**SCHEDULE 2-2**

**THE ORDERED GOODS, SERVICE LEVELS AND SERVICE CREDITS**

**1. INTRODUCTION**

1.1 This Schedule 2-2 specifies:

1.1.1 the Ordered Goods and Ordered Services;

1.1.2 the Service Levels applicable to each of the Ordered Goods and Ordered Services; and

1.1.3 the Service Credits applicable where Service Levels are not met.

**2. THE ORDERED GOODS AND SERVICES**

**2.1 General**

2.1.1 The CONTRACTOR shall provide, operate and support an application, licensing, contact management and business information system on behalf of the CUSTOMER as a fully managed service. This will include:

2.1.1.1 Workflow system and management;

2.1.1.2 Operation of Contact Centre operations;

2.1.1.3 Document handling (receipt, scanning, storage);

2.1.1.4 Licence application processing;

2.1.1.5 Payment processing;

2.1.1.6 Competence checking of applicants by reference to external awarding bodies;

2.1.1.7 Criminality checking with the Criminal Records Bureau (CRB), Disclosure Scotland or Access Northern Ireland;

2.1.1.8 Physical Licence Distribution including Card Production and Destruction Services

2.1.1.9 Security – ensuring the service meets the requirements for “Restricted” data. This covers people, processes and technology aspects;

2.1.1.10 Business continuity – provision of disaster recovery facilities, and continuity Strategies;

2.1.1.11 Service management – providing full 24x7x365 service and support

**2.2 The Ordered Goods**

2.2.1 **Ordered Goods** shall comprise:

2.2.1.1 Items used for the processing and issue of the Application and manufacture of the Licence including:

(a) Envelopes

(b) Paper

(c) Cards

(d) Lanyards

(e) Card Holders

**2.3 The Ordered Services are defined in paragraphs 2.4 to 2.42 below.**

**2.4 Document handling inbound**

- 2.4.1 Opening post, scanning, OCR of application forms; valuables and indexing of all scanned documents. Pre-Validation that all required valuables have been supplied and can be processed.

**2.5 Submit applications**

- 2.5.1 The CONTRACTOR to provide services and application solution for Security Operatives and Security Operators to submit applications for a Licence, so they can legally operate within the Private Security Industry. The CUSTOMER requires the Applicant to apply by paper or electronically and to be able to track the status of that Application's progress. Security Operatives can apply independently or via a Company Sponsor who manages the submission of Applications on behalf of their employees. A Licence has to be renewed prior to expiry to enable the Security Operative to operate within the regulations.

2.5.2 The CONTRACTOR shall:

- 2.5.2.1 manage the design and publication of Application forms for individual SIA Licences.
- 2.5.2.2 provide a Solution that supports changes to the Application form structure and data content with minimal impact on re-design, testing and implementation. Minimal impact defined as no detrimental change on business as usual with regards to service availability and processing times.
- 2.5.2.3 provide a Solution to enable an individual to register as a Company Sponsor.
- 2.5.2.4 provide a Solution to enable a lead Company Sponsor to manage the approval, amendment and deletion of other sponsors for their company.
- 2.5.2.5 provide a Solution to enable an Applicant to amend a previously submitted Application and re-submit to CUSTOMER.
- 2.5.2.6 provide a Solution for an Applicant or Company Sponsor to register for web based facilities.
- 2.5.2.7 provide a Solution to verify an Applicant or Company Sponsor is registered for access to web based facilities.
- 2.5.2.8 provide a Solution for an Applicant to track the status of their Application.
- 2.5.2.9 provide a Solution for a Company Sponsor to track the Application status and fee details for Applications they have submitted.
- 2.5.2.10 provide a Solution to enable the generation of an online Application to prepare for submission to the CUSTOMER.
- 2.5.2.11 provide a Solution to enable a Company Sponsor to generate an online Application on behalf of the Applicant.

---

## ICT GOODS AND ASSOCIATED SERVICES

---

- 2.5.2.12 provide a Solution that enables a Company Sponsor to submit multiple online Applications in one transaction.
- 2.5.2.13 provide a Solution for registered web users to save and retrieve a partially completed online Application.
- 2.5.2.14 provide a Solution to print a completed Application/s locally (e.g. at home or place of work).
- 2.5.2.15 provide a Solution to print a partially completed Application locally.
- 2.5.2.16 provide a Solution to print the completed Application centrally.
- 2.5.2.17 provide a Solution to enable an Applicant to apply for Licences for one or more Licensable Activities in a single Application.
- 2.5.2.18 provide a Solution with an integrated self-help facility for completing online Applications.
- 2.5.2.19 provide a Solution for a Company Sponsor to define a list of Licence Holders to track the status of each Licence.

### **2.6 Receive & distribute mail items**

#### **2.6.1 The CONTRACTOR shall:**

- 2.6.1.1 receive and distribute all correspondence (general mail items and Applications) on behalf of the CUSTOMER.
- 2.6.1.2 receive all mail items addressed to the CUSTOMER post boxes.
- 2.6.1.3 provide a Solution to stream mail received by mail category (currently defined by post box number).
- 2.6.1.4 provide a Solution to distribute mail items addressed to specific individuals within CUSTOMER.
- 2.6.1.5 provide a Solution to create an electronic image of selected mail items received for the CUSTOMER.
- 2.6.1.6 provide a Solution to record the return of a SIA Licence Card against the Licence Holder.
- 2.6.1.7 provide a Solution to securely destroy returned SIA Licence Cards.
- 2.6.1.8 manage the return of documents to the Applicant or Company Sponsor.
- 2.6.1.9 provide a Solution that records all Supporting Evidence that is returned to the Applicant or Company Sponsor.
- 2.6.1.10 provide a Solution that records the date the documents are returned to the Applicant or Company Sponsor.
- 2.6.1.11 provide a Solution to securely return valuable Identity Documents to Applicants or their Company Sponsors.
- 2.6.1.12 provide a Solution for the CUSTOMER and the Applicant to track the delivery of valuable Identity Documents.
- 2.6.1.13 shall provide a Solution to retain all mail items for an agreed period (currently 6 months).

---

## ICT GOODS AND ASSOCIATED SERVICES

---

- 2.6.1.14 provide a Solution to destroy all mail items after a period to be agreed with the CUSTOMER (currently 6 months).
- 2.6.1.15 provide a Solution to print, prepare and despatch all required outgoing mail items.
- 2.6.1.16 provide a Solution to record and retrieve content of all mail items despatched.
- 2.6.1.17 provide a Solution to print, prepare and despatch Disclosure Request Forms for Criminal Records Bureau & Disclosure Scotland & Access NI.
- 2.6.1.18 provide a Solution to record the date each mail item was despatched.
- 2.6.1.19 provide a Solution that links incoming mail to an Application, Licence Holder or contact.
- 2.6.1.20 provide a Solution to distribute electronic images of mail received to the addressees or teams responsible for the mail items.

### 2.7 Handle application documents

#### 2.7.1 The CONTRACTOR shall:

- 2.7.1.1 manage the transfer of paper Applications, Disclosure Returns and Supporting Evidence documentation into electronic format.
- 2.7.1.2 provide a Solution to record the date an Application package is received.
- 2.7.1.3 provide a Solution to record the evidence documents received with an Application.
- 2.7.1.4 provide a Solution to link a Manual Payment Transaction with the Application being paid for.
- 2.7.1.5 provide a Solution to link all Applications funded by one payment.
- 2.7.1.6 provide a Solution to link all Applications submitted by a Company Sponsor.
- 2.7.1.7 provide a Solution to create an electronic image of a Disclosure Return received from the Criminal Records Bureau, Disclosure Scotland or Access Northern Ireland.
- 2.7.1.8 provide a Solution to store paper Applications and Supporting Evidence received from Applicants during the Application process.

### 2.8 Capture data

#### 2.8.1 The CONTRACTOR shall:

- 2.8.1.1 capture the electronic Application and Disclosure Return data and verify the data against the paper forms and correct where necessary.
- 2.8.1.2 a Solution to digitise the data provided in an Application form for a SIA Licence.
- 2.8.1.3 provide a Solution to create an electronic image of the photograph provided with the Application form .

## ICT GOODS AND ASSOCIATED SERVICES

---

- 2.8.1.4 provide a Solution to link Application data to a known Applicant or Licence Holder.
- 2.8.1.5 provide a Solution to automatically link Disclosure Return data to a known Applicant or Licence Holder.
- 2.8.1.6 provide a Solution to verify the digitised data captured matches the data provided in the Application form.
- 2.8.1.7 provide a Solution to create an Application Case.
- 2.8.1.8 provide a Solution to link the Application Case to an existing Applicant or Licence Holder.
- 2.8.1.9 provide a Solution to mark an Application Case where an Applicant has declared Criminality on the Application form.
- 2.8.1.10 provide a Solution to mark an Application Case where a Mental Health Issue is reported on the Application form.
- 2.8.1.11 provide a Solution to create an electronic image of all Supporting Evidence submitted.
- 2.8.1.12 provide a Solution to verify the digitised data matches the data on Supporting Evidence submitted with an Application.
- 2.8.1.13 provide a Solution to identify potentially fraudulent Identity Documents.
- 2.8.1.14 provide a Solution to integrate existing Document Authentication Technology with the data capture Solution.
- 2.8.1.15 provide a Solution to check the integrity and authenticity of manual documents received for confirming identity, in accordance with CUSTOMER Identity Document standards.
- 2.8.1.16 provide a Solution to refer potentially fraudulent documents to the CUSTOMER for investigation.
- 2.8.1.17 provide a Solution to link together Multiple Application records received from a Company Sponsor.

### 2.9 Validate application

#### 2.9.1 The CONTRACTOR shall:

- 2.9.1.1 provide a Solution to validate Applications received. The CUSTOMER validation rules for re-submission & renewals & Secondary Licence Applications may vary depending on the Supporting Evidence previously held on the CUSTOMER systems. The CONTRACTOR is required to communicate with the Applicant or Company Sponsor to gather the missing information and complete the validation stage.
- 2.9.1.2 provide a Solution to check each Application form received is fully and correctly completed according to the CUSTOMER Guidance Notes.
- 2.9.1.3 provide a Solution to identify Applications that have mandatory items missing.

## ICT GOODS AND ASSOCIATED SERVICES

- 
- |          |   |
|----------|---|
| 2.9.1.4  | provide a Solution to check the photographic image received with the Application is to the required standard and signed and dated by a valid counter signatory.   |
| 2.9.1.5  | provide a Solution to identify Supporting Evidence that does not meet the CUSTOMER Identity Document standards.   |
| 2.9.1.6  | provide a Solution to check the Applicant's address history to identify an Application that requires an Overseas Criminality Certificate according to CUSTOMER Licensing Criteria.                          |
| 2.9.1.7  | provide a Solution that provides an option to allow a Licence Application requiring an Overseas Criminality Certificate to continue beyond the validation stage, for subsequent assessment by the CUSTOMER. |
| 2.9.1.8  | provide a Solution to check the Supporting Evidence received is correct and relates to the Applicant.   |
| 2.9.1.9  | provide a Solution to check valid payment details have been received with the Application.  |
| 2.9.1.10 | provide a Solution to verify cheque, postal order & bankers draft details.  |
| 2.9.1.11 | provide a Solution to check the age of the Applicant meets the SIA Licensing Criteria.  |
| 2.9.1.12 | provide a Solution to reject Applications that are incomplete or incorrect.   |
| 2.9.1.13 | provide a Solution to record a rejection reason for an Application received as incorrect or incomplete.   |
| 2.9.1.14 | provide a Solution to notify the Applicant about the rejection of their Application and the reasons for rejection.  |
| 2.9.1.15 | provide a Solution to notify the Company Sponsor about the rejection of Applications they have submitted.   |
| 2.9.1.16 | provide a Solution to confirm a Company Sponsor submitting Multiple Applications is an approved Company Sponsor.  |
| 2.9.1.17 | provide a Solution to communicate with the Applicant that their Application has been accepted.  |
| 2.9.1.18 | provide a Solution to resolve a validation error with the Applicant.  |
| 2.9.1.19 | provide a Solution to Case Note an Application with the resolution to an error.   |
| 2.9.1.20 | provide a Solution to progress the CUSTOMER authorised Identity Document Exemption cases through an agreed set of validation rules (agreed with the Applicant).   |
| 2.9.1.21 | provide a Solution to confirm change of circumstance details received for an Applicant are correct and complete (change of name, change of address, change of photo, change of signature).                  |
| 2.9.1.22 | provide a Solution that updates the status of an Application Case following rejection or acceptance.  |
-

**2.10 Licence application processing**

- 2.10.1 Back office processing of the application request with external bodies e.g. CRB/SCRO and Awarding Bodies. Progression of an application to the point where a decision can be made.

**2.11 Establish eligibility**

**2.11.1 The CONTRACTOR shall:**

- 2.11.1.1 provide a Solution that proves the Applicant is eligible to hold an SIA Licence for the Licensable Activity they wish to operate in.
- 2.11.1.2 provide a Solution to support the completion of Eligibility Checks according to the SIA Licensing Criteria.
- 2.11.1.3 provide a Solution to enable Awarding Bodies to import multiple Applicant qualification details & Supporting Evidence (including photographic image & signature for each Applicant) to a central qualifications database.
- 2.11.1.4 provide a Solution to enable Awarding Bodies to import Supporting Evidence as required to meet the CUSTOMER identity checks.
- 2.11.1.5 provide a Solution to enable Awarding Bodies to import qualification details including date of assessment.
- 2.11.1.6 provide a Solution to notify Awarding Bodies when the import of qualification details is unsuccessful
- 2.11.1.7 provide a Solution to check the existence of an Applicant's valid and current qualification where necessary on a central datastore.
- 2.11.1.8 provide a Solution to check whether an Applicant holds a suitable qualification for the Licensable Activity they are applying for, in accordance with the CUSTOMER Competency Rules.
- 2.11.1.9 provide a Solution to check whether an Applicant holds a suitable qualification and top-up certificate in accordance with the SIA Competency Rules.
- 2.11.1.10 provide a Solution that responds to changes in qualification classifications and their validity with minimal impact on the managed service Solution and business change function.
- 2.11.1.11 provide a Solution to manage the receipt and decision of an Identity Document Exemption request.
- 2.11.1.12 provide a Solution to verify the identity of the Applicant is the same as the identity of the person completing the qualification.
- 2.11.1.13 provide a Solution that interfaces with the Identity and Passport Service Passport Verification Service to retrieve the Applicant's UK passport photo & signature from the Identity and Passport Service, for comparison against the photo & signature received with their Application.

## ICT GOODS AND ASSOCIATED SERVICES

---

- 2.11.1.14 provide a Solution that uses the Identity and Passport Service Passport Verification Service to retrieve on request the Applicant's UK passport photo & signature from the Identity and Passport Service, for comparison against the photo & signature received with their Application.
- 2.11.1.15 provide a Solution to enable Authorised SIA Staff to remove incorrectly matched identity records.
- 2.11.1.16 provide a Solution that checks the photo & signature held with their qualification matches the photo & signature received with their Application.
- 2.11.1.17 provide a Solution that refers an Application to the CUSTOMER when the passport record is retrieved with Defined Issues.
- 2.11.1.18 provide a Solution that has the capability to automatically retrieve the countersignatory's UK passport photo & signature from the Identity and Passport Service.
- 2.11.1.19 provide a Solution to retrieve on request the countersignatory's UK passport photo & signature from the Identity and Passport Service.
- 2.11.1.20 provide a Solution to check the validity of the UK passport held for the Applicant's counter signatory.
- 2.11.1.21 provide a Solution to generate and submit Disclosure Requests via an automated interface to the Criminal Records Bureau depending on the residential post code and address history of the Applicant.
- 2.11.1.22 provide Solution to generate & submit Disclosure Requests to the Criminal Records Bureau, depending on the residential post code and address history of the Applicant.
- 2.11.1.23 provide a Solution to generate & submit Disclosure Requests to Disclosures Scotland, depending on the residential post code and address history of the Applicant.
- 2.11.1.24 provide a Solution to generate & submit Disclosure Requests to Access Northern Ireland, depending on the residential post code and address history of the Applicant.
- 2.11.1.25 provide a Solution to generate & submit Disclosure Requests to Access Northern Ireland, for all Applicants with a Republic of Ireland residential post code.
- 2.11.1.26 provide a Solution to retrieve an automated response from the Criminal Records Bureau relating to an Applicant's Criminality.
- 2.11.1.27 provide a Solution that adds an electronic image of signature and relevant details of the CUSTOMER counter-signatory to the Disclosure Request form.
- 2.11.1.28 provide a Solution to assess the Disclosure Return based on the Criminality information provided in the Disclosure Return.
- 2.11.1.29 provide a Solution to resolve issues with Disclosure Requests from Criminal Records Bureau, Disclosure Scotland and Access NI.

## ICT GOODS AND ASSOCIATED SERVICES

---

- 2.11.1.30 provide a Solution to enable Authorised SIA Staff to assess the Criminality included in the Disclosure Return against the SIA Licensing Criteria.
- 2.11.1.31 provide a Solution to assess any declared Criminality included in the Application against the SIA Licensing Criteria.
- 2.11.1.32 provide a Solution to reconcile Disclosure Request and Disclosure Returns.
- 2.11.1.33 provide a Solution to enable Authorised SIA Staff to assess any Overseas Criminality Certificate or sworn oath received with an Application, against the SIA Licensing Criteria.
- 2.11.1.34 provide a Solution to enable Authorised SIA Staff to request a Right To Work check with UK Border Agency.
- 2.11.1.35 provide a Solution to store the results of a Right To Work check from UK Border Agency against an Applicant or Licence Holder.
- 2.11.1.36 provide a Solution that avoids duplication of Right To Work checks for Applicants where a further Right To Work check is not required or the check is currently in progress.
- 2.11.1.37 provide a Solution to provide an audit trail of all requests submitted and all results received of Right To Work checks to and from UK Border Agency.
- 2.11.1.38 provide a Solution to identify outstanding Right To Work results not received n days after request.
- 2.11.1.39 provide a Solution to manage the investigation into mental health, where there is a record of Mental Health Issues declared in the Application.
- 2.11.1.40 provide a Solution that alerts Authorised SIA Staff when an Application with a Mental Health Issue is declared.
- 2.11.1.41 provide a Solution that alerts Authorised SIA Staff to Applications that have related conviction or Non-conviction information.
- 2.11.1.42 provide a Solution that prevents Applications that have related conviction or Non-conviction information progress to Licensing Decision.
- 2.11.1.43 provide a Solution that generates a risk score against each Application received based on new and existing information stored relating to the Applicant.
- 2.11.1.44 provide a Solution that enables Authorised SIA Staff to set and maintain parameters to establish a risk score.
- 2.11.1.45 provide a Solution that enables Authorised SIA Staff to set & maintain the rules for determining a risk score.
- 2.11.1.46 provide a Solution that alerts Authorised SIA Staff when an Application breaches the threshold of acceptable risk.
- 2.11.1.47 provide a Solution that prevents the Application from progressing to Licensing Decision based on the risk score achieved.

- 2.11.1.48 provide a Solution that enables Authorised SIA Staff to progress the Application to Licensing Decision based on the assessment of the risk score achieved.
- 2.11.1.49 provide a Solution that enables Authorised SIA Staff to record the outcome of the assessment of the risk score.

## 2.12 Making SIA licence decision

### 2.12.1 The CONTRACTOR shall:

- 2.12.1.1 provide a Solution to support the decision making for SIA Licences.
- 2.12.1.2 provide a Solution that streams Applications for decision making according to the results of the Eligibility Checks.
- 2.12.1.3 provide a Solution that streams complete Applications for decision making to different groups of staff within the CUSTOMER organisation.
- 2.12.1.4 provide a Solution to enable Authorised SIA Staff to review the Licence Application Case to make a decision to grant or refuse a Licence. Authorised SIA Staff will need access to all relevant previous & current Application Case history and previous + current Licence details.
- 2.12.1.5 provide a Solution that records the result of the Licensing Decision against the Application Case.
- 2.12.1.6 provide a Solution that records details of the Authorised SIA Staff making the Licensing Decision.
- 2.12.1.7 provide a Solution that enables an Application Case to be put on hold whilst further information is collected to support the Licensing Decision.
- 2.12.1.8 provide a Solution that enables Authorised SIA Staff to change the status of an Application to 'Minded to Refuse'.
- 2.12.1.9 provide a Solution that enables Authorised SIA Staff to record a reason for refusal.
- 2.12.1.10 provide a Solution that changes the status of an Application at 'Minded to Refuse' to 'Refused' after n days from date of decision, if no Appeal is received.
- 2.12.1.11 provide a Solution that enables Authorised SIA Staff to grant a Licence.
- 2.12.1.12 provide a Solution that enables Authorised SIA Staff to refuse a Licence.
- 2.12.1.13 provide a Solution that enables Authorised SIA Staff to notify the Applicant of the Licensing and the reason for the decision.
- 2.12.1.14 provide a Solution that enables a Case Note to be made against an Applicant or Application Case.

- 2.12.1.15 provide a Solution that enables Authorised SIA Staff to review all previous Licensing Decisions for the Applicant or Licence Holder, to assess the quality of the decision made by CUSTOMER staff.
- 2.12.1.16 provide a Solution that requires user confirmation of the Licensing Decision.
- 2.12.1.17 provide a Solution that manages the updates to the Public Register of Licence Holders with each new Licence granted.

### **2.13 Manage appeals**

2.13.1 The CONTRACTOR to provide a Solution to manage the Pre-Appeal and Appeals process in cases where a Licence is refused, a Licence is revoked or a Licence is suspended.

2.13.2 The CONTRACTOR shall:

- 2.13.2.1 provide a Solution to manage the Pre-Appeal and Appeal process for SIA Licences.
- 2.13.2.2 provide a Solution to support the Appeals process in different courts, including but not limited to magistrate, sheriff and crown courts.
- 2.13.2.3 provide a Solution to link a response to a Licensing Decision to an Application Case.
- 2.13.2.4 provide a Solution to enable Authorised SIA Staff to review the response to a Licensing Decision for each Application Case.
- 2.13.2.5 provide a Solution to enable Authorised SIA Staff to change a Licensing Decision, based on the response to the Licensing Decision.
- 2.13.2.6 provide a Solution to enable Authorised SIA Staff to generate correspondence with the Applicant during the Appeals process.
- 2.13.2.7 provide a Solution to manage the progression of an Appeal throughout the Appeals process.
- 2.13.2.8 provide a Solution to enable Authorised SIA Staff to notify the Applicant of the outcome of the Appeal.
- 2.13.2.9 provide a Solution to automatically uphold the Licensing Decision when there is no response from the Applicant within n days.
- 2.13.2.10 provide a Solution to prevent automatic change of Application or Licence status when a response to a Licensing is received.
- 2.13.2.11 provide a Solution to record the reason for the outcome of the Appeal.
- 2.13.2.12 provide a Solution that enables Authorised SIA Staff to review previous Appeal decisions to assess the quality of the decision made.

### **2.14 Maintain SIA license**

2.14.1 The CONTRACTOR shall:

- 2.14.1.1 provide a Solution to manage the changes to Licence and Licence Holder details due to change of circumstances such as change of address, name or photo.
- 2.14.1.2 provide a Solution to manage the reporting of lost, stolen or damaged Licence Cards and replaced cards as required.
- 2.14.1.3 provide a Solution to manage the changes to the status of a SIA Licence and Licence Holder over its lifetime, this includes, revoking, suspending and re-instating a Licence. The change in status of a SIA Licence needs to be reflected on the SIA Public Register of Licence Holders.

## **2.15 Change of circumstances**

### **2.15.1 The CONTRACTOR shall:**

- 2.15.1.1 provide a Solution to manage the change of circumstances to the information held relating to the Licence Holder and their Licence.
- 2.15.1.2 provide a Solution to manage the change in address details held for the Licence Holder.
- 2.15.1.3 provide a Solution to confirm proof of address using the Supporting Evidence provided, in accordance with the CUSTOMER change of address policy.
- 2.15.1.4 provide a Solution to update the new address for the Licence Holder.
- 2.15.1.5 provide a Solution to notify the Licence Holder of their updated address details and return any Supporting Evidence.
- 2.15.1.6 provide a Solution to manage the notification of a change in appearance of a Licence Holder.
- 2.15.1.7 provide a Solution to verify the Licence Holder from previously supplied evidence.
- 2.15.1.8 provide a Solution to update the photographic image held for the Licence Holder.
- 2.15.1.9 provide a Solution to replace the Licence Card with a new photo.
- 2.15.1.10 provide a Solution to update the Public Register of Licence Holders with verified change in circumstances.
- 2.15.1.11 provide a Solution to refer to the exceptional change of circumstances e.g. gender change, signature change without name change.
- 2.15.1.12 provide a Solution to manage the change in name details held for the Licence Holder.
- 2.15.1.13 provide a Solution to verify the change of name against the Supporting Evidence in accordance with CUSTOMER change of name policy.
- 2.15.1.14 provide a Solution to update the verified change of name for the Licence Holder.

- 2.15.1.15 provide a Solution to notify the Licence Holder of their updated name details and return any Supporting Evidence.
- 2.15.1.16 provide a Solution to issue a replacement Licence Card with new name.
- 2.15.1.17 provide a Solution to capture and validate the Licence Holder's new signature on change of name.
- 2.15.1.18 provide a Solution to escalate to the CUSTOMER any suspicious change in circumstance or replacement Licence requests.
- 2.15.1.19 provide a Solution to manage the notification of lost or stolen Licence Cards.
- 2.15.1.20 provide a Solution for a Licence Holder to report a lost, stolen or damaged Licence Card.
- 2.15.1.21 provide a Solution to verify the Licence status and case history prior to issuing a replacement Licence Card.
- 2.15.1.22 provide a Solution to receive and securely destroy returned damaged Licence Cards.
- 2.15.1.23 provide a Solution to manage the replacement or re-issue of Licence Cards.
- 2.15.1.24 provide a Solution to record the notification of death of a Licence Holder.
- 2.15.1.25 provide a Solution to verify the death of the Licence Holder against a Death Certificate.
- 2.15.1.26 provide a Solution to stop all correspondence with a Licence Holder on notification of death.
- 2.15.1.27 provide a Solution to cancel the SIA Licence on verified notification of death.
- 2.15.1.28 provide a Solution manage change of circumstance details received from Applicants (change of name, change of address, change of photo, change of signature) in relation to their Application, prior to licence decision.

## **2.16 Change of license status**

### **2.16.1 The CONTRACTOR shall:**

- 2.16.1.1 provide a Solution to manage the change of Licence status.
- 2.16.1.2 provide a Solution to notify the Licence Holder of the change in status of their SIA Licence.
- 2.16.1.3 provide a Solution to refer updates from the Licence Holder relating to their Licence Conditions.
- 2.16.1.4 provide a Solution for Authorised SIA Staff to reject Suspension & Revocation requests and record a reason for rejection.
- 2.16.1.5 provide a Solution to enable Authorised SIA Staff to respond to SIA Intelligence requested actions with outcome and reasons.

- 2.16.1.6 provide a Solution to enable Authorised SIA Staff with appropriate authority to change a Licence status.
- 2.16.1.7 provide a Solution that enables Authorised SIA Staff to review any information held for a Licence Holder to consider a change in Licence status.
- 2.16.1.8 provide a Solution that enables Authorised SIA Staff to allocate a reason for Suspension or Revocation.
- 2.16.1.9 provide a Solution to receive and record returned Licence Cards for suspended & revoked Licences.
- 2.16.1.10 provide a Solution to identify Suspension cases ready for review (currently after 90 days from Suspension, when no response or update has been received).
- 2.16.1.11 provide a Solution to allocate a reason for Reinstatement for the Licence.
- 2.16.1.12 provide a Solution to allocate a reason for a change in status to 'Minded to Revoke'.
- 2.16.1.13 provide a Solution to automatically change a status from 'Minded to Revoke' to 'Revoked' after n days where no Pre-Appeal or Appeal has been received. (currently 42 days)
- 2.16.1.14 provide a Solution to notify the Licence Holder of the automatic change in Licence status and the need to return their Licence Card to the CUSTOMER.
- 2.16.1.15 provide a Solution to automatically update the status of a Licence on the Public Register of Licence Holders.
- 2.16.1.16 provide a Solution that enables Authorised SIA Staff to review a change in Licence status decisions and rejections to assess the quality of the decision made.
- 2.16.1.17 provide a Solution to identify Licence Holders where the recorded Right To Work has expired prior to the Licence expiry.
- 2.16.1.18 provide a Solution to request a re-check of the Licence Holder's Right To Work.

## **2.17 SIA license expiry**

### **2.17.1 The CONTRACTOR shall:**

- 2.17.1.1 provide a Solution to inform a Licence Holder that their Licence is approaching expiry and provide information to support their renewal.
- 2.17.1.2 provide a Solution to change the status of a Licence on expiry.
- 2.17.1.3 provide a Solution to update the Public Register of Licence Holders with the expiry of a Licence.

## **2.18 Manage complaints & compensation**

- 2.18.1 The CONTRACTOR is required to provide a Solution to manage the first point of contact for resolution of complaints, comments & enquiries.

2.18.2 The CONTRACTOR shall:

- 2.18.2.1 provide a Solution to manage the receipt and resolution to complaints, comments & enquiries received into the CUSTOMER.
- 2.18.2.2 provide a Solution to record all responses to complaints, comments & enquiries.
- 2.18.2.3 provide a Solution to allocate a classification against each complaint, comment and enquiry received.
- 2.18.2.4 provide a Solution to refer and escalate a complaint, comment or enquiry to the CUSTOMER based on the classification.
- 2.18.2.5 provide a Solution to escalate a complaint, comment or enquiry to the CUSTOMER when required.
- 2.18.2.6 provide a Solution that creates a subject record where there has been no previous contact with the CUSTOMER.
- 2.18.2.7 provide a Solution that links the complaint, comment or enquiry to the subject.
- 2.18.2.8 provide a Solution that generates a unique reference number for each complaint, comment or enquiry case.
- 2.18.2.9 provide a Solution to log the user responsible for responding to each complaint, comment & enquiry received.
- 2.18.2.10 provide a Solution to review the complaint, comment & enquiry case history.

**2.19 Withdraw application**

2.19.1 The CONTRACTOR shall:

- 2.19.1.1 provide a Solution to withdraw an Application. An Application is withdrawn once payment is received, on the request of the Applicant or when considered appropriate by an Authorised SIA Staff member. There are no refunds for Applications withdrawn.
- 2.19.1.2 provide a Solution to withdraw an Application.
- 2.19.1.3 provide a Solution for Authorised SIA Staff to re-activate a withdrawn Application.
- 2.19.1.4 provide a Solution to notify the Applicant their Application has been withdrawn.
- 2.19.1.5 provide a Solution to record the reason for the withdrawal.

**2.20 Manage Intelligence**

2.20.1 The CONTRACTOR shall:

- 2.20.1.1 manage the receipt and dissemination of Intelligence Information into and from the CUSTOMER.
- 2.20.1.2 provide a Solution to managed the receipt of Intelligence Information gathered via the Contact Centre and CrimeStoppers
- 2.20.1.3 provide a Solution to incorporate a method for marking Applicants, their Applications and Business related data for monitoring purposes.

**2.21 Payment processing and accounting**

2.21.1 Taking of payments from individuals and company sponsors. Reconciliation of bulk payments against valid applications received. Monthly, Quarterly and Annual financial reporting.

**2.22 Taking payment**

2.22.1 The CONTRACTOR shall:

- 2.22.1.1 manage the receipt, payment, payment reconciliation & refunds for all the SIA Licences. The Application fee is non-refundable.
- 2.22.1.2 provide a Solution to collect payment from an Applicant using the credit & debit card details provided with the Application.
- 2.22.1.3 provide a Solution to refund overpayment following n days from Manual Payment Transaction receipt, where overpayment is greater than an agreed limit.
- 2.22.1.4 provide a Solution to collect manual payments (cheque, postal order, bankers draft).
- 2.22.1.5 provide a Solution that applies discounted fees for Applicants previously licensed according to the CUSTOMER Application fees policy.
- 2.22.1.6 provide a Solution to log a payment received against the related Application.
- 2.22.1.7 provide a Solution to bank all Manual Payment Transactions on behalf of the CUSTOMER.
- 2.22.1.8 provide a Solution to resolve a payment error with the Applicant or Company Sponsor prior to notification.
- 2.22.1.9 provide a Solution to Case Note an Application with the resolution to a payment error.
- 2.22.1.10 provide a Solution to add a Case Note to all payment activity for an Application.
- 2.22.1.11 provide adequate controls on the payments service to ensure proper auditing of payments management.
- 2.22.1.12 provide a Solution to collect the full Application fee amount from the Applicant where the Manual Payment Transaction received is insufficient.
- 2.22.1.13 ensure that an Application is placed on hold until full payment is received.
- 2.22.1.14 provide a Solution to enable a Company Sponsor to make a single payment for Multiple Applications.
- 2.22.1.15 provide a Solution to enable a Company Sponsor to set up a direct debit mandate to recover payment for Multiple Applications.
- 2.22.1.16 provide a Solution to initiate direct debit payment for Multiple Applications.

- 2.22.1.17 provide a Solution to report to the Company Sponsor the Application fees that are covered by a single payment.
- 2.22.1.18 provide a Solution to report to the Company Sponsor the fees refunded and the Applications relevant to the refund.
- 2.22.1.19 provide a Solution that enables a change in licence fee with minimal impact on the managed service Solution and business change functions.

## **2.23 Manage service delivery finance**

### **2.23.1 The CONTRACTOR shall:**

- 2.23.1.1 provide a Solution to support the management and accounting for the CUSTOMER fees income.
- 2.23.1.2 provide a Solution to reconcile payment transactions against the relevant bank statement by income stream and payment method, on a daily basis.
- 2.23.1.3 provide a Solution that provides access to CUSTOMER income transactions for third parties (e.g. auditors) as authorised by the CUSTOMER.
- 2.23.1.4 provide a Solution to transfer fee income received to the SIA HQ bank account at a frequency to be agreed with the CUSTOMER (currently 4th & 9th working day of the month).
- 2.23.1.5 provide notification of all Manual Payment Transactions by type received that have not cleared the supplier account at the relevant accounting month end.
- 2.23.1.6 provide notification of all automated payment transactions by type received that have not cleared the supplier account at the relevant accounting month end.
- 2.23.1.7 provide notification of all payments received for SIA Licences at accounting month end.
- 2.23.1.8 provide notification of all outstanding debts for SIA Licences at accounting month end.
- 2.23.1.9 provide notification of all refunds made for SIA Licences at accounting month end.

## **2.24 Manage service finance**

### **2.24.1 The CONTRACTOR shall:**

- 2.24.1.1 manage the finances relating to the development and provision of the managed service Solution.
- 2.24.1.2 provide essential financial management information to the SIA at a frequency to be agreed with the CUSTOMER.
- 2.24.1.3 confirm with the CUSTOMER the charging principles, the method for apportioning of fixed costs, chargeable and non-chargeable items and the basis for making charges at a frequency to be agreed with the CUSTOMER.

- 2.24.1.4 develop, publish and distribute a catalogue for chargeable items at a frequency to be agreed with the CUSTOMER.
- 2.24.1.5 accumulate base charging data and at a frequency to be agreed with the CUSTOMER, calculate invoices, charges and statements for the services provided.
- 2.24.1.6 follow standard procurement protocols for the provision of goods & services to support the managed service Solution.

## **2.25 Manage business intelligence reporting**

2.25.1 The CONTRACTOR is required to provide a Solution to support business intelligence reporting within CUSTOMER. Business intelligence reports are required for strategic and operational performance, and day to day team management.

2.25.2 The CONTRACTOR shall:

- 2.25.2.1 provide a Solution that includes definition and delivery of a range of reports to manage and report on CUSTOMER business operational performance.
- 2.25.2.2 provide a Solution that enables scheduling of reporting on an hourly/daily/ weekly/monthly/quarterly & annual basis.
- 2.25.2.3 provide a Solution that is capable of reporting on real-time activities within the supplier and CUSTOMER operations.
- 2.25.2.4 provide a Solution that alerts the supplier and CUSTOMER staff when performance issues are identified during real time monitoring of key activities.
- 2.25.2.5 provide a Solution that supports reporting of key activities completed within the managed service Solution by an individual.

## **2.26 Client enquiry management**

2.26.1 Handling inbound calls, emails, faxes and web based tracking of applications, renewals and other details both using live agents and automated response systems such as IVR, E-Mail Wizards and Web based Forms and Services.

## **2.27 Manage contacts**

2.27.1 The CONTRACTOR shall:

- 2.27.1.1 provide a Contact Centre service to manage calls and related communications to the CUSTOMER. The CUSTOMER receives contact and communication from a wide spectrum of people including; potential Applicants, Licence Holders, Company Sponsors, Enforcement Partners, MPs and members of the public. The CONTRACTOR is expected to receive and respond to communications from various sources using industry standard channels (phone, email, letter & fax).
- 2.27.1.2 provide a Contact Centre service that is available to receive and respond to contacts from 8am - 8pm, Monday - Friday, excluding Bank Holidays.

## ICT GOODS AND ASSOCIATED SERVICES

---

- 2.27.1.3 provide a Contact Centre to support calls to and from potential Applicants, Applicants, Licence Holders, Company Sponsors, Approved Contractors, MPs, members of the public and Enforcement Partners.
- 2.27.1.4 provide a Self Service Facility to support Call Centre activity, including but not limited to: requesting brochures & Application forms, tracking of Application progress, access to Public Registers and web registration services.
- 2.27.1.5 provide a Solution to enable an Applicant or Company Sponsor to cancel an Application (prior to taking payment).
- 2.27.1.6 provide a Solution to notify the Applicant that cancellation was successful.
- 2.27.1.7 provide a Solution to respond to a caller's enquiry relating to the CUSTOMER, it's services, policies & procedures.
- 2.27.1.8 provide a Solution to respond to a complaint relating to the CUSTOMER, it's services, policies, procedures and Licence Holders.
- 2.27.1.9 provide a Solution to enable user registration for web based services.
- 2.27.1.10 provide a Solution to enable a user to maintain their registration for web based services.
- 2.27.1.11 provide a Solution to enable a Company Sponsor to be registered with the CUSTOMER.
- 2.27.1.12 provide a Solution to provide a 'call back' facility where further investigation is required to resolve a caller's enquiry or complaint.
- 2.27.1.13 provide a Solution to verify the identity of the caller with information currently stored within the CUSTOMER systems.
- 2.27.1.14 provide a Solution to manage fulfilment requests for brochures, Application forms and other marketing material on behalf of the CUSTOMER.
- 2.27.1.15 provide a Solution to distribute brochures, Application forms and other marketing material on behalf of the CUSTOMER.
- 2.27.1.16 provide a Solution to refer offers of Intelligence Information to the CrimeStoppers service.
- 2.27.1.17 provide a Solution to receive Intelligence Information and refer the Intelligence Information to the CUSTOMER Intelligence Team in an agreed format.
- 2.27.1.18 provide a Solution to refer requests for information under the Freedom of Information Act or Data Protection Act to the CUSTOMER for action.
- 2.27.1.19 provide a Solution that enables callers to the Contact Centre to look-up entries on the SIA Public Register of Licence Holders.
- 2.27.1.20 provide a Solution that enables Applicants & Company Sponsors to track the status of their Application/s.

- 2.27.1.21 provide a Solution to receive and respond to communications by industry standard channels; email, letter, fax, phone.
- 2.27.1.22 provide a Solution to record the resolution of each customer contact and record the content of all outgoing communications.
- 2.27.1.23 provide a Solution to record and store all oral communications to the Contact Centre and make recordings of all communications available to the CUSTOMER for playback.
- 2.27.1.24 provide a Solution to enable callers to call the Contact Centre using the CUSTOMER local rate phone number/s.

2.27.2 The Contact Centre telephone numbers (presently 0844 892 1025) will remain the property of the CUSTOMER.

## **2.28 Print production and postage**

- 2.28.1 Batch printing and posting of all process generated mail.

## **2.29 Card production**

- 2.29.1 The secure production and destruction of license badges on behalf of the SIA.

## **2.30 Produce SIA licence package**

- 2.30.1 The CONTRACTOR to personalise and issue Licence Cards and Licence letters.
- 2.30.2 The CONTRACTOR shall:
  - 2.30.2.1 provide a Solution to print & personalise SIA Licence Cards for Front Line Staff.
  - 2.30.2.2 provide a Solution to print SIA Licence Cards that identify the Licensable Activity the Licence is for.
  - 2.30.2.3 provide a Solution to add name, Licence number, photographic image, signature and expiry date to the SIA Licence Card.
  - 2.30.2.4 provide a Solution to record the date the SIA Licence Card was printed.
  - 2.30.2.5 provide a Solution to generate a SIA Licence Card issue letter for Front Line staff.
  - 2.30.2.6 provide a Solution to generate a Licence issue letter for Non-Front Line staff.
  - 2.30.2.7 provide a Solution to collate the printed SIA Licence Card and Licence issue letter ready for despatch.
  - 2.30.2.8 provide a secure environment to protect the access to, and distribution of non-personalised SIA Licence Cards.

## **2.31 Despatch SIA licence package**

- 2.31.1 The Licence Card, letter and related materials are sent to the Licence Holder or Company Sponsor.
- 2.31.2 The CONTRACTOR shall:
  - 2.31.2.1 provide a Solution to despatch the Licence Card package to the Licence Holder, for next day delivery.

2.31.2.2 provide a Solution to despatch Licence packages in unbranded envelopes.

2.31.2.3 provide a Solution to cancel a Licence and halt the despatch of a Licence package on the instruction of Authorised SIA Staff.

## **2.32 ICT infrastructure**

2.32.1 Provision of end-to-end technical solution. Support and maintenance of ICT solution.

## **2.33 Manage solution development**

2.33.1 The CONTRACTOR will provide 90 man days for the ICT solution developments per annum. The SIA may submit a request to change the size of the team, which will result in a pro-rata change in the Fixed Monthly charge in accordance with the agreed rates. Any such change will be incorporated via the Change Control Procedure. Change Control Notes that require the use of the ICT Development resources will be raised on the basis that the first cumulative 90 man days per month will be free of charge.

2.33.2 The CONTRACTOR shall:

2.33.2.1 manage the development of the managed service Solution throughout the lifetime of the contract.

2.33.2.2 participate in the joint definition, establishment and agreement of the managed service Solution strategy and architecture where it is required to do so by the CUSTOMER.

2.33.2.3 communicate internally the managed service Solution strategy & architecture and ensure internal conformance with these to the standards agreed with the CUSTOMER.

2.33.2.4 review the managed service Solution strategy & architecture in the light of new technology, new services proposed or developed, changes to business strategy, or changes to IT strategy.

2.33.2.5 bring any required changes in these areas, together with an impact assessment of these changes, to the attention of the CUSTOMER and in agreement with the CUSTOMER carry out the ongoing maintenance of these as required.

2.33.2.6 ensure that all necessary hardware installations, upgrades or other changes are implemented to ensure that service delivery targets are maintained.

## **2.34 Systems maintenance**

2.34.1 The CONTRACTOR shall:

2.34.1.1 manage the maintenance of the managed service Solution throughout the lifetime of the contract.

2.34.1.2 design and develop a Solution that identifies duplicate data entry and alerts the user.

2.34.1.3 maintain the tracking and distribution of software/vendor documentation, software updates, and licenses for all managed service Solution users.

## ICT GOODS AND ASSOCIATED SERVICES

---

- 2.34.1.4 manage software licenses and coordinate with users to determine if licenses are still required and ensure that required software licenses do not expire.
- 2.34.1.5 provide full hardware maintenance and support services required to enable the functioning of the Managed Service Configuration Items.
- 2.34.1.6 perform routine preventive maintenance on Managed Service Configuration Items.
- 2.34.1.7 resolve or manage the resolution by third party manufacturers of Problems with Configuration Items within the managed service Solution.
- 2.34.1.8 procure or carry out the necessary maintenance of the Configuration Items within the managed service Solution.
- 2.34.1.9 provide LAN/WAN support services within the main data centre, regional environments and reserve facilities.
- 2.34.1.10 manage and monitor wide area network connections where necessary to deliver the services outlined in the contract.
- 2.34.1.11 ensure software support is in place for all software supplied, to agreed service levels.

### 2.35 **Manage service desk**

#### 2.35.1 The CONTRACTOR shall:

- 2.35.1.1 provide a Service Desk capability to support development and use of the managed service Solution.
- 2.35.1.2 provide a Service Desk to include a single point of contact for the managed service Solution users to report Incidents, request information and request services.
- 2.35.1.3 provide Service Desk support via a number of channels to include but not limited to; phone support, remote support, fax/email and onsite support.
- 2.35.1.4 manage calls to the service desk from receipt through to closure, maintaining communication with all parties involved, including the CUSTOMER and any internal or external organisations involved.
- 2.35.1.5 provide full service desk support during the agreed service availability (8am - 6pm Monday to Friday) excluding Bank Holidays

### 2.36 **Manage service availability**

#### 2.36.1 The CONTRACTOR shall:

- 2.36.1.1 manage the availability of services provided.
- 2.36.1.2 provide and maintain a secure online service management document library, available 24 hours a day, 7 days a week.
- 2.36.1.3 provide availability of the managed service Solution to the CUSTOMER from 8am - 8pm, Monday - Friday, excluding Bank Holidays.

## ICT GOODS AND ASSOCIATED SERVICES

---

- 2.36.1.4 provide availability of the managed service Solution to CUSTOMER staff to support planned operations (out of normal office hours).
- 2.36.1.5 provide availability of web-based services 24 hours a day, 7 days a week.
- 2.36.1.6 monitor the performance and operation of all Configuration Items agreed in the contract.
- 2.36.1.7 create and maintain availability plans for all services, systems and critical components included in the contract.
- 2.36.1.8 collect operational data relating to the availability of services, systems and critical components included in the contract for the purposes of availability management.
- 2.36.1.9 ensure that the service availability meets the Service Level Agreement targets.
- 2.36.1.10 monitor and report the actual availability achieved of services, systems and critical components against the CUSTOMER, and shall initiate remedial action as and where necessary.
- 2.36.1.11 announce scheduled service unavailability and anticipated downtime to the CUSTOMER.
- 2.36.1.12 agree scheduled service unavailability and anticipated downtime with the CUSTOMER.
- 2.36.1.13 develop and agree in consultation, processes for the announcement and notification of scheduled and unscheduled service unavailability.
- 2.36.1.14 notify unscheduled service unavailability and anticipated downtime to the CUSTOMER as soon as it is discovered.
- 2.36.1.15 re-test the availability plan at every major change to the managed service Solution.

### **2.37 Manage service capacity**

#### **2.37.1 The CONTRACTOR shall:**

- 2.37.1.1 manage the capacity of the services provided.
- 2.37.1.2 ensure that capacity is available at all times to meet the CUSTOMER's business need.
- 2.37.1.3 develop and maintain systems that provide sufficient systems capacity to meet changing licensing demand during the lifetime of the contract.
- 2.37.1.4 ensure that service quality complies with the service levels as defined in the Service Level Agreement.
- 2.37.1.5 develop and maintain systems that will measure and report on transaction load and systems capacity.
- 2.37.1.6 ensure there is sufficient data storage capacity to manage CUSTOMER business needs for all systems deployed as part of the managed service Solution.

**2.38 Manage Incidents**

**2.38.1 The CONTRACTOR shall:**

- 2.38.1.1 manage Incidents as they occur within the managed service Solution.
- 2.38.1.2 provide a means for managing Incidents to include methods for recording, prioritising and classifying the Incident so it can be scaled appropriately according to the existing or negotiated service level agreement.
- 2.38.1.3 escalate Incidents that are out of their control to the appropriate party.
- 2.38.1.4 keep the CUSTOMER informed of the progress relating to all Incidents.
- 2.38.1.5 perform periodic analysis of Incident trends, identifying repeat Incidents and Incidents that are re-opened, reporting on action to be taken to prevent their reoccurrence, raising Problem records as appropriate.
- 2.38.1.6 produce formal response to severe Incidents (as defined by the CUSTOMER), cataloguing the nature of the Incident, the cause and those actions that are recommended / required to be taken to avoid any further recurrence.
- 2.38.1.7 ensure that all staff involved in Incident management have access to relevant information such as known errors, Problem resolution and the configuration management library.
- 2.38.1.8 provide a defined process to classify and manage major Incidents, in agreement with the CUSTOMER.
- 2.38.1.9 consult with the CUSTOMER to establish the initial diagnosis of Incidents that affect shared services or infrastructure.
- 2.38.1.10 resolve Incidents according to their classification within agreed service levels.

**2.39 Manage problems**

**2.39.1 The CONTRACTOR shall:**

- 2.39.1.1 manage Problem resolution.
- 2.39.1.2 provide a Problem management capability to include methods for recording common Incidents, known errors and identifying and managing the introduction of Solutions.
- 2.39.1.3 raise a Problem record as a result of an Incident or set of similar Incidents whose root cause was/were not known at the time of service recovery or Incident closure.
- 2.39.1.4 raise a Problem record after recognising a pattern of similar or associated Incidents.
- 2.39.1.5 agree the severity and impact of each Problem with the CUSTOMER.

- 2.39.1.6 lead the investigation and diagnosis of the Problem and communicate progress to the CUSTOMER and other parties as appropriate.
- 2.39.1.7 resolve Problems, communicate resolution details, submitting Service Change Requests as appropriate.
- 2.39.1.8 update Problem records after resolution with known error details.
- 2.39.1.9 ensure changes required in order to correct the underlying cause of Problems are entered in to the SIA Change Management process.
- 2.39.1.10 monitor Problem resolution, reviewing and reporting on its effectiveness to the CUSTOMER.
- 2.39.1.11 ensure Problem management provides up-to-date information on known errors and corrected Problems for updating Incident management.
- 2.39.1.12 ensure that actions for improvement identified during the resolution of Problems are recorded and input into a plan for improving the service.
- 2.39.1.13 resolve Problems within agreed Service Levels.

#### **2.40 Manage service configuration**

##### **2.40.1 The CONTRACTOR shall:**

- 2.40.1.1 maintain a Configuration Management Library of configurable items for the managed service Solution.
- 2.40.1.2 provide a means for Configuration Management to detail the IT infrastructure components and associated assets. This should detail any interdependencies to allow impact analysis for future changes to the service.
- 2.40.1.3 maintain an asset register for all Configuration Items including hardware and software supported within the contract & share with the SIA document library.
- 2.40.1.4 report the status of all service related inventory, configuration and assets at a frequency to be agreed with the CUSTOMER.
- 2.40.1.5 ensure that the degree of control on Configuration Items is sufficient to meet the business needs, acceptable risk of failure and service criticality.
- 2.40.1.6 ensure that Configuration Management provides information to the Change Management process on the impact of a requested change on the service or Configuration Item.
- 2.40.1.7 ensure that changes to Configuration Items shall be traceable and auditable where appropriate, e.g. for changes and movements of software and hardware.
- 2.40.1.8 ensure a baseline of the appropriate Configuration Items shall be taken before a release to the live environment.

- 2.40.1.9 ensure that master copies of digital Configuration Items are controlled in secure physical or electronic libraries and referenced to the configuration records, e.g. software, testing products, support documents.
- 2.40.1.10 ensure all Configuration Items are uniquely identifiable.
- 2.40.1.11 ensure the status of Configuration Items, their versions, location, related changes and Problems and associated documentation are visible to those who require it.
- 2.40.1.12 ensure that configuration audit procedures include recording deficiencies, initiating corrective actions and reporting on the outcome.

#### **2.41 Manage business continuity**

##### **2.41.1 The CONTRACTOR shall:**

- 2.41.1.1 provide a disaster recovery and continuity management plan for all services provided in accordance with Schedule 2-14.
- 2.41.1.2 securely manage all aspects of backup and recovery for the managed service Solution.
- 2.41.1.3 ensure there are appropriate backup and restore policies and that the capabilities are implemented. This must include testing of the restore process, testing and checking the backups, appropriate storage and protection of backup media.
- 2.41.1.4 provide contingency planning and disaster recovery management for systems, to agreed service levels

#### **2.42 Manage third party suppliers**

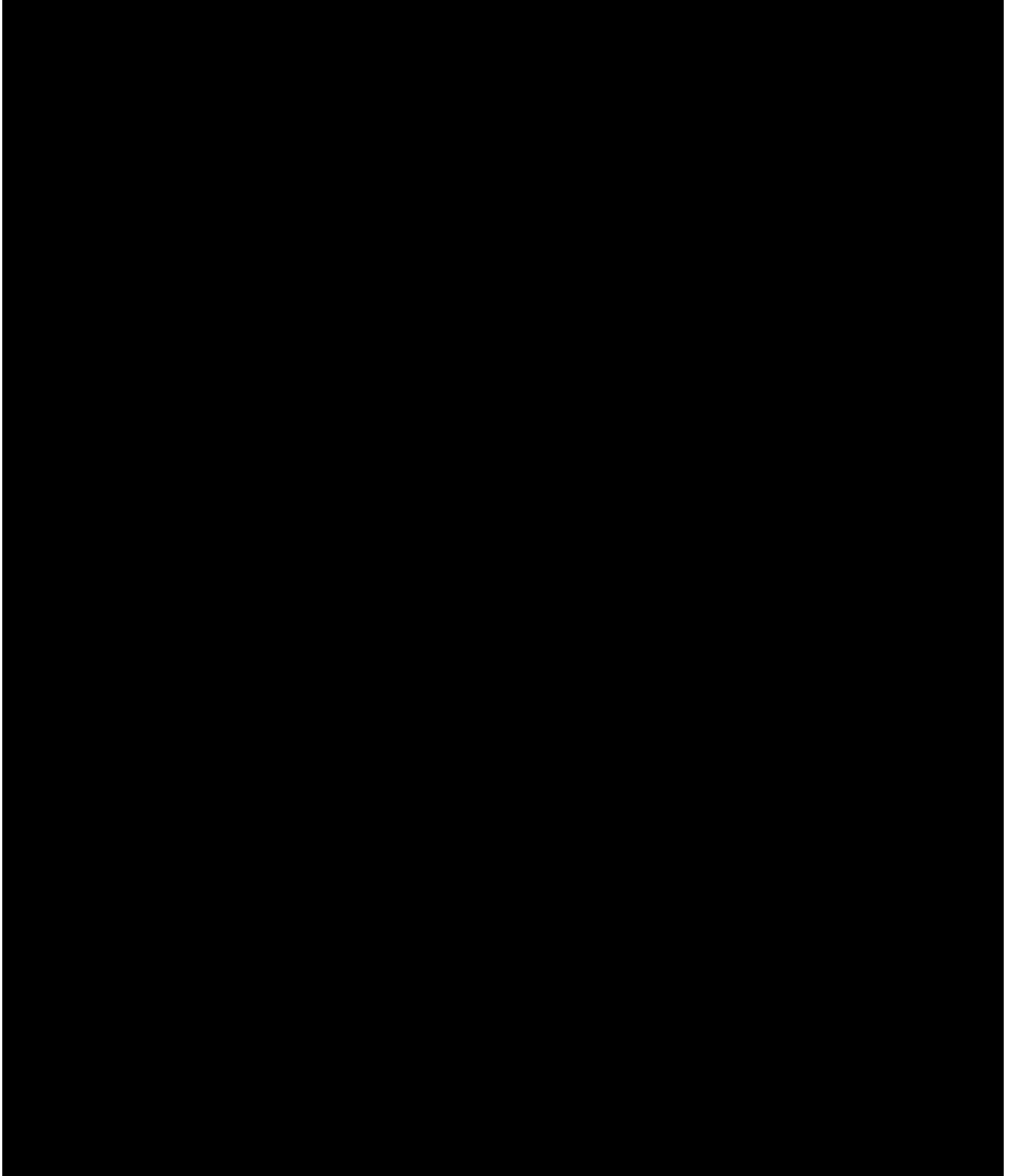
##### **2.42.1 The CONTRACTOR shall:**

- 2.42.1.1 manage the relationship with any third party suppliers who are engaged in providing the managed service Solution.
- 2.42.1.2 document third party supplier management processes for all subcontractors utilised.
- 2.42.1.3 name a Contract Manager responsible for each third party supplier.
- 2.42.1.4 define clear service boundaries with other third party suppliers through a Memorandum of Understanding or similar formal agreement.
- 2.42.1.5 ensure that services to be provided by the third party supplier(s) are documented in SLAs or other documents agreed by all parties. This should include, but not be limited to requirements, scope, level of service and communication processes.
- 2.42.1.6 ensure that SLAs agreed with third party suppliers align with those of the CUSTOMER.
- 2.42.1.7 carry out regular reviews of any services subcontracted to third parties incorporating third party performance reporting into their overall service performance report as required by the CUSTOMER.

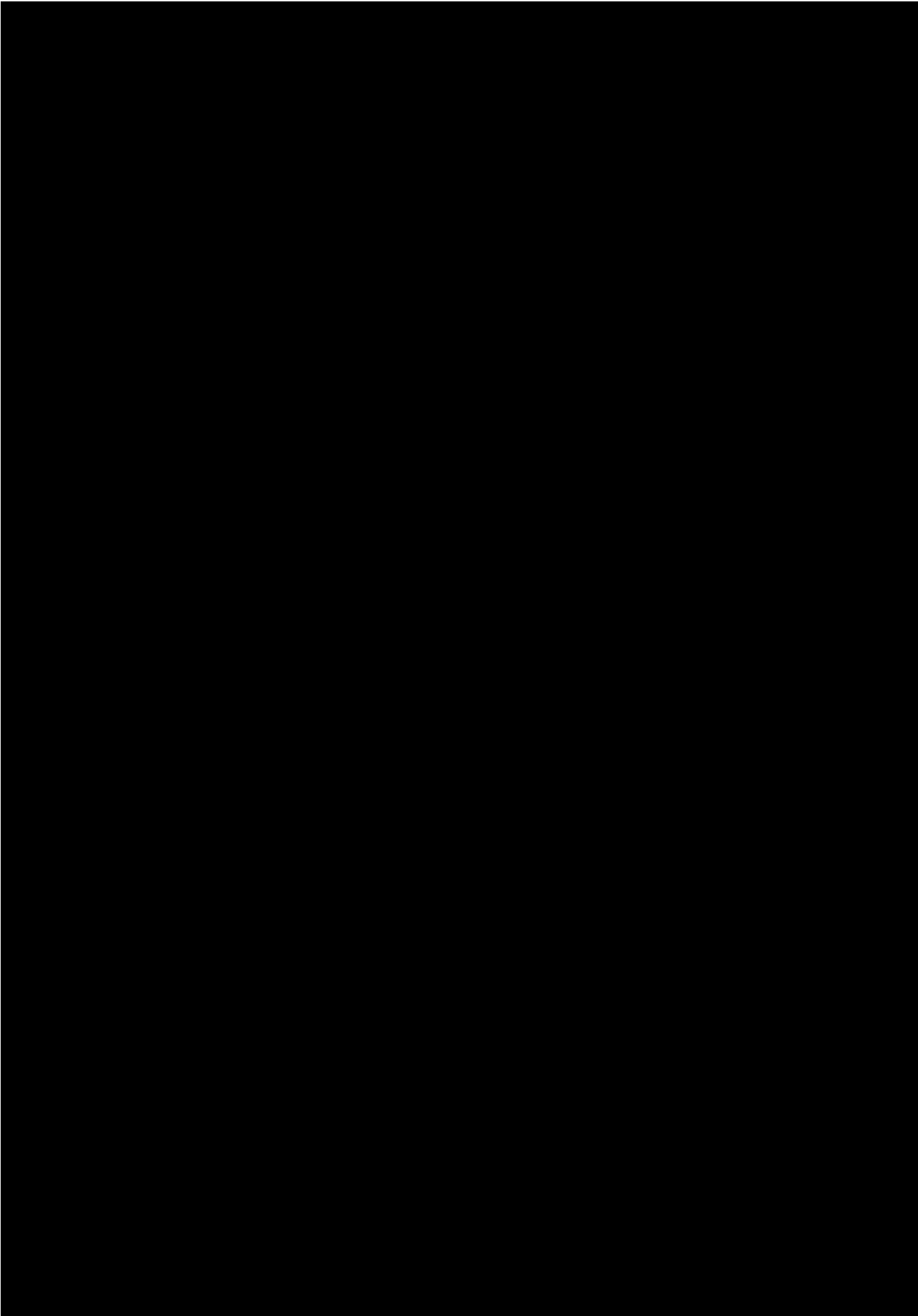
## ICT GOODS AND ASSOCIATED SERVICES

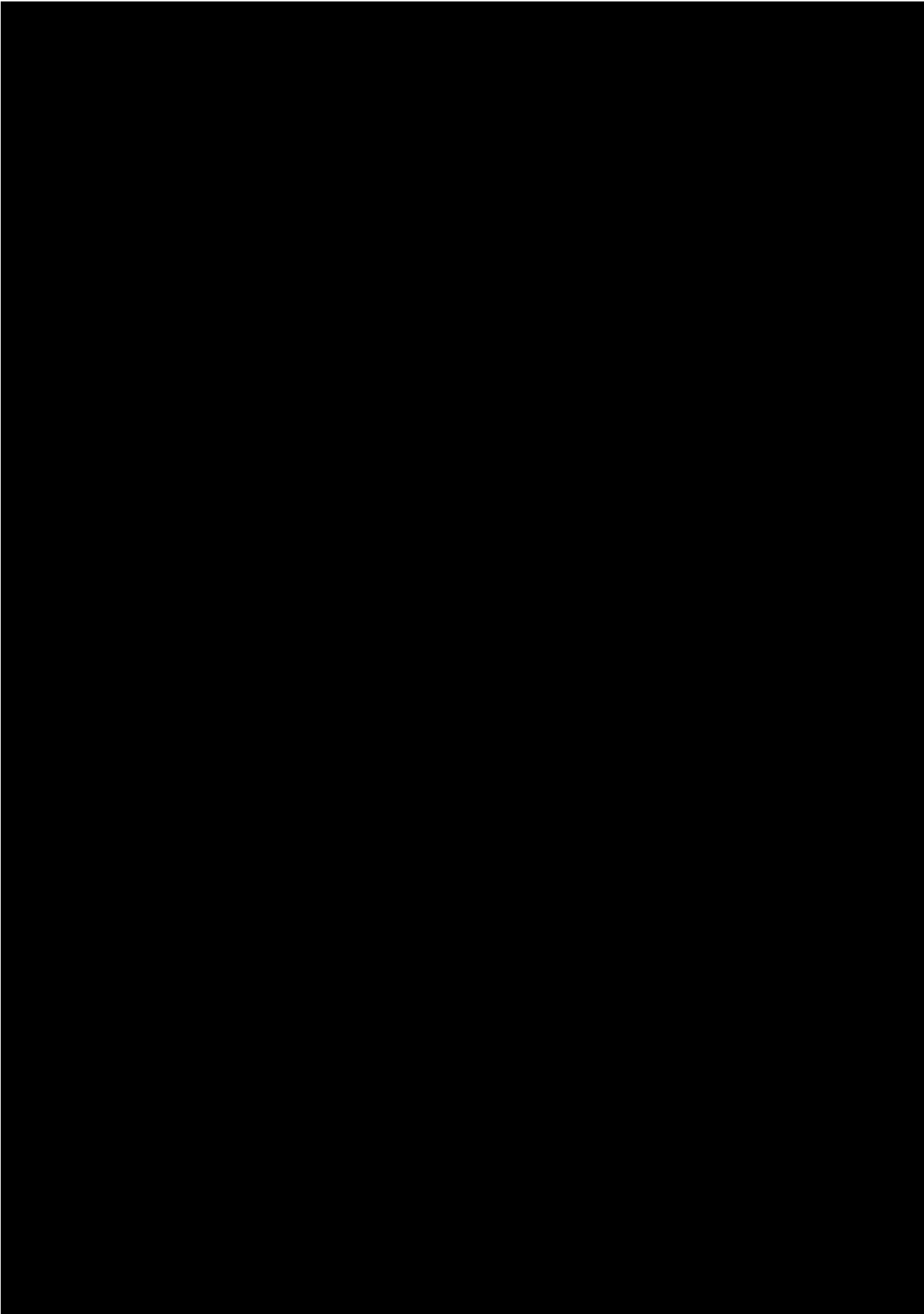
---

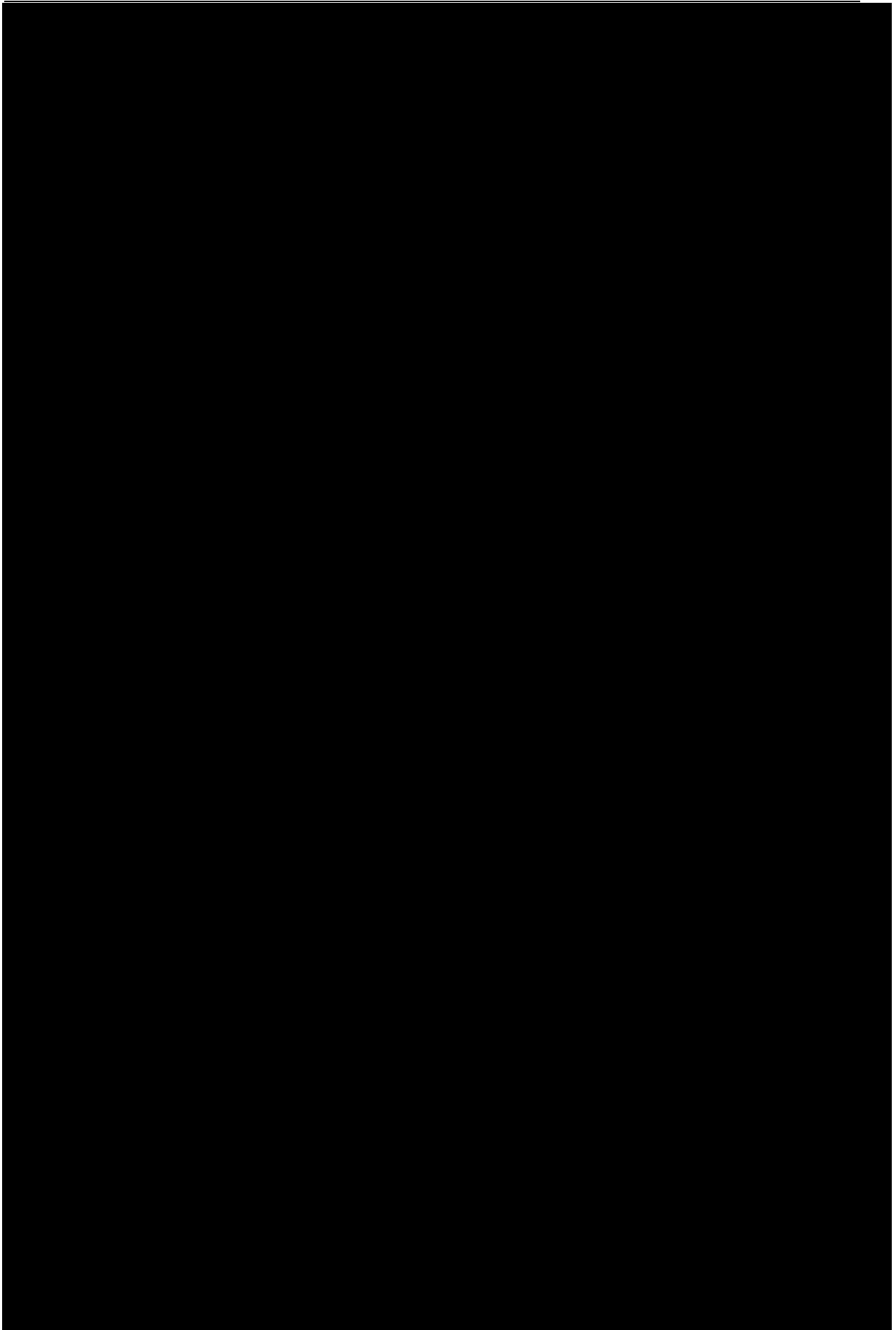
- 2.42.1.8 ensure that a process is in place for a major review of the contract or formal agreement (with the third Party Supplier) at least annually to ensure that business needs and contractual obligations are still being met.
- 2.42.1.9 provide representatives to attend the Business Improvement Group (BIG) to discuss improvements to the managed service provision.
- 2.42.1.10 use all available information to provide input into a plan for improving the service and that plan will be managed by BIG.

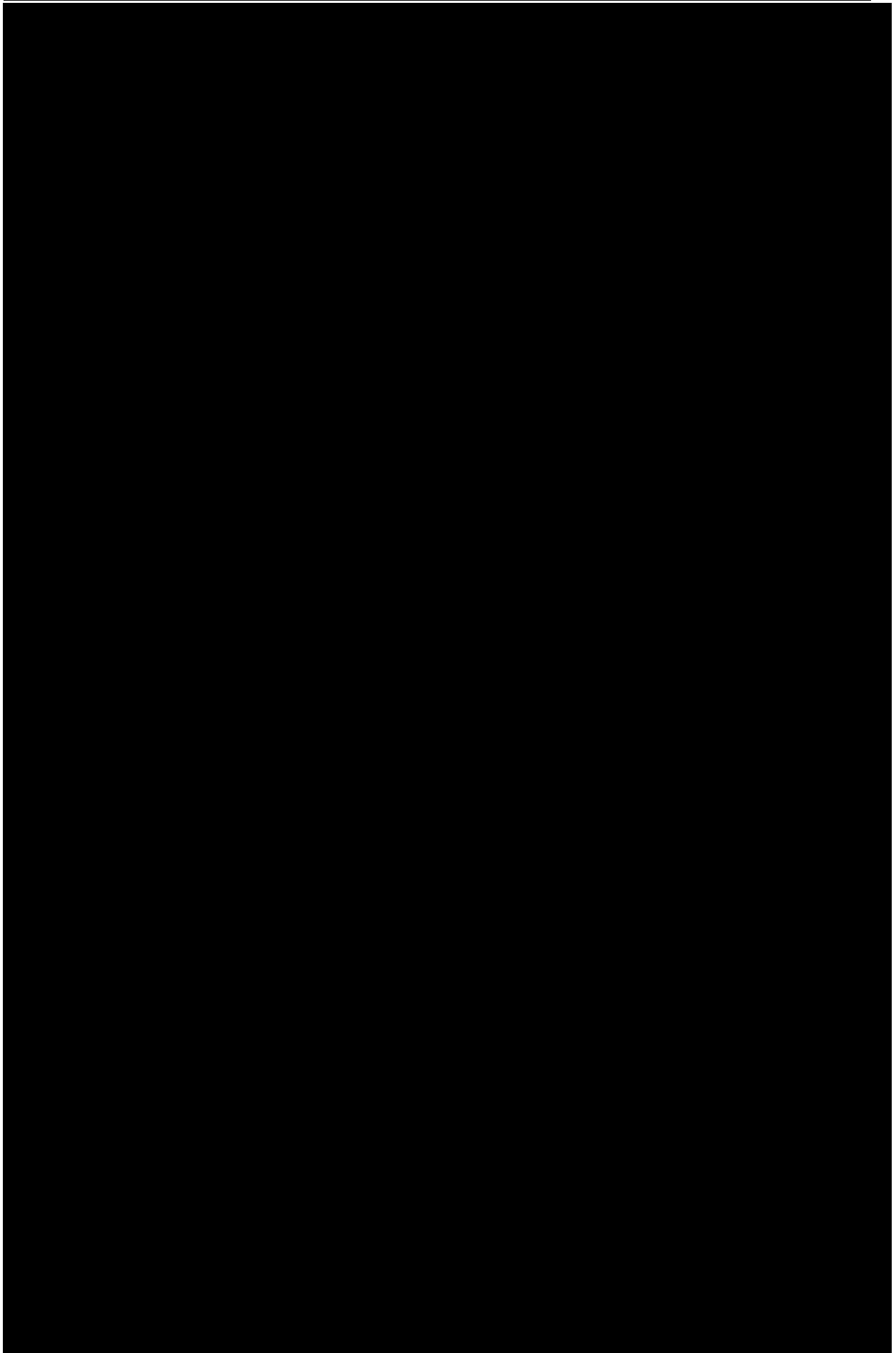


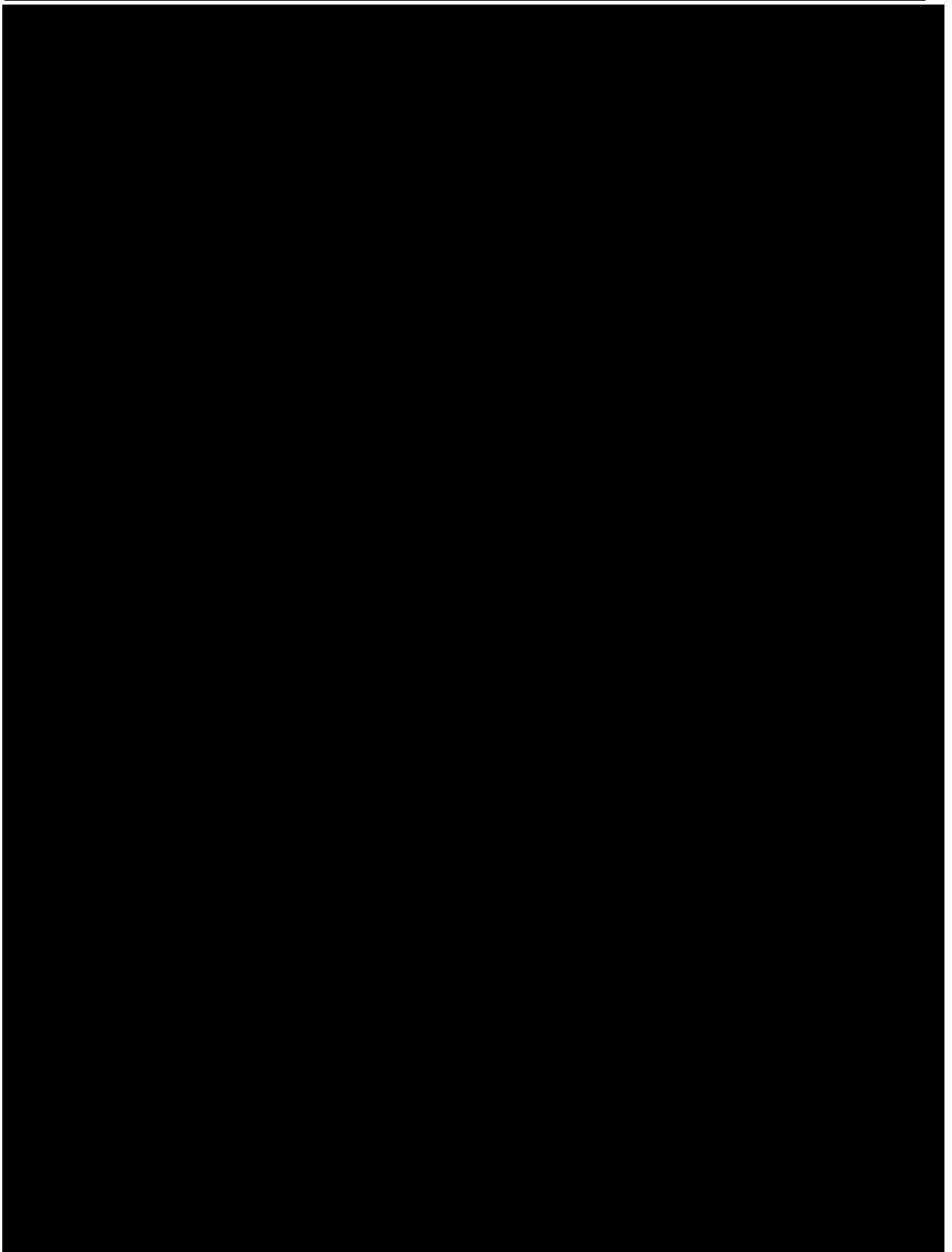






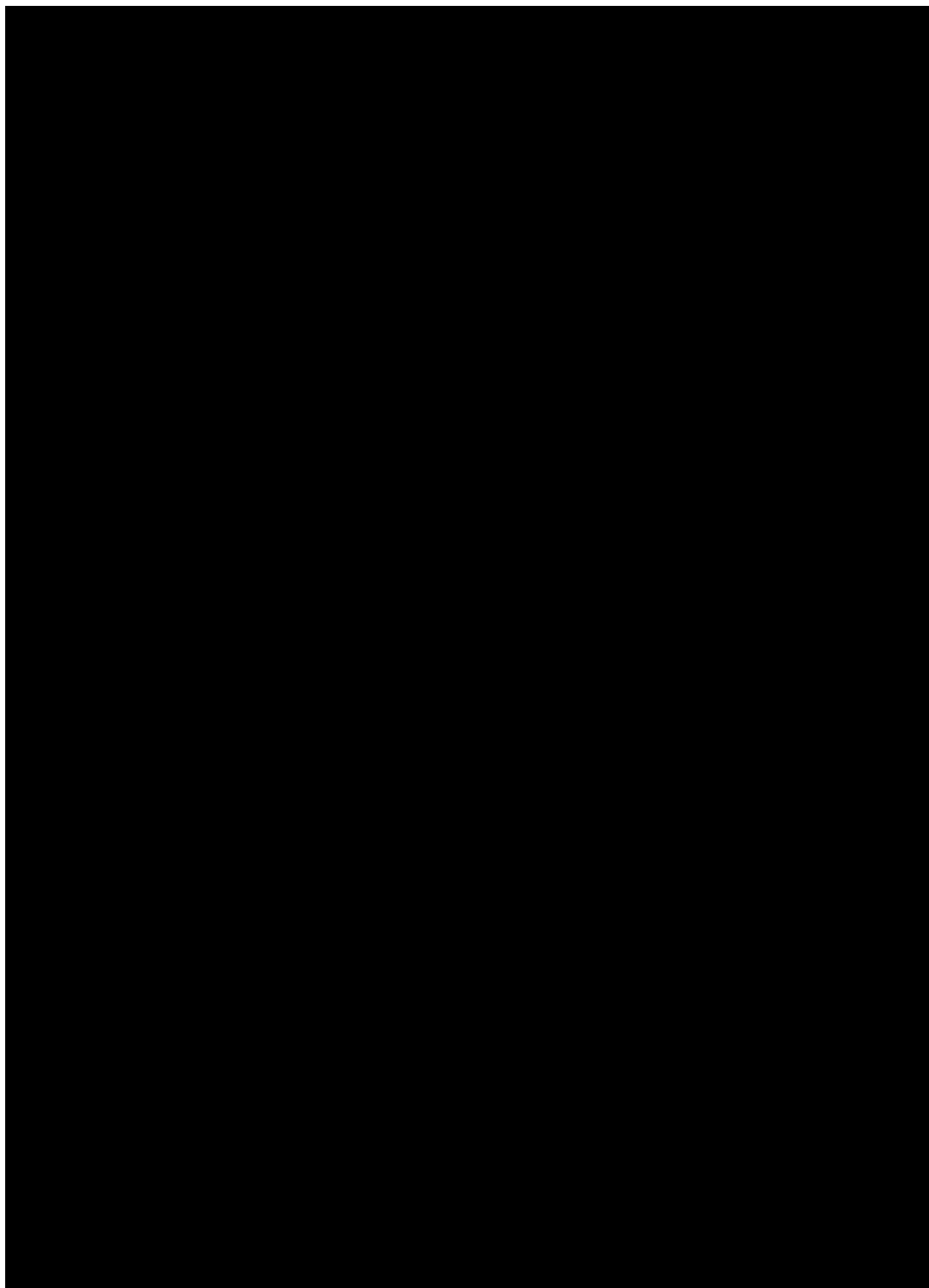


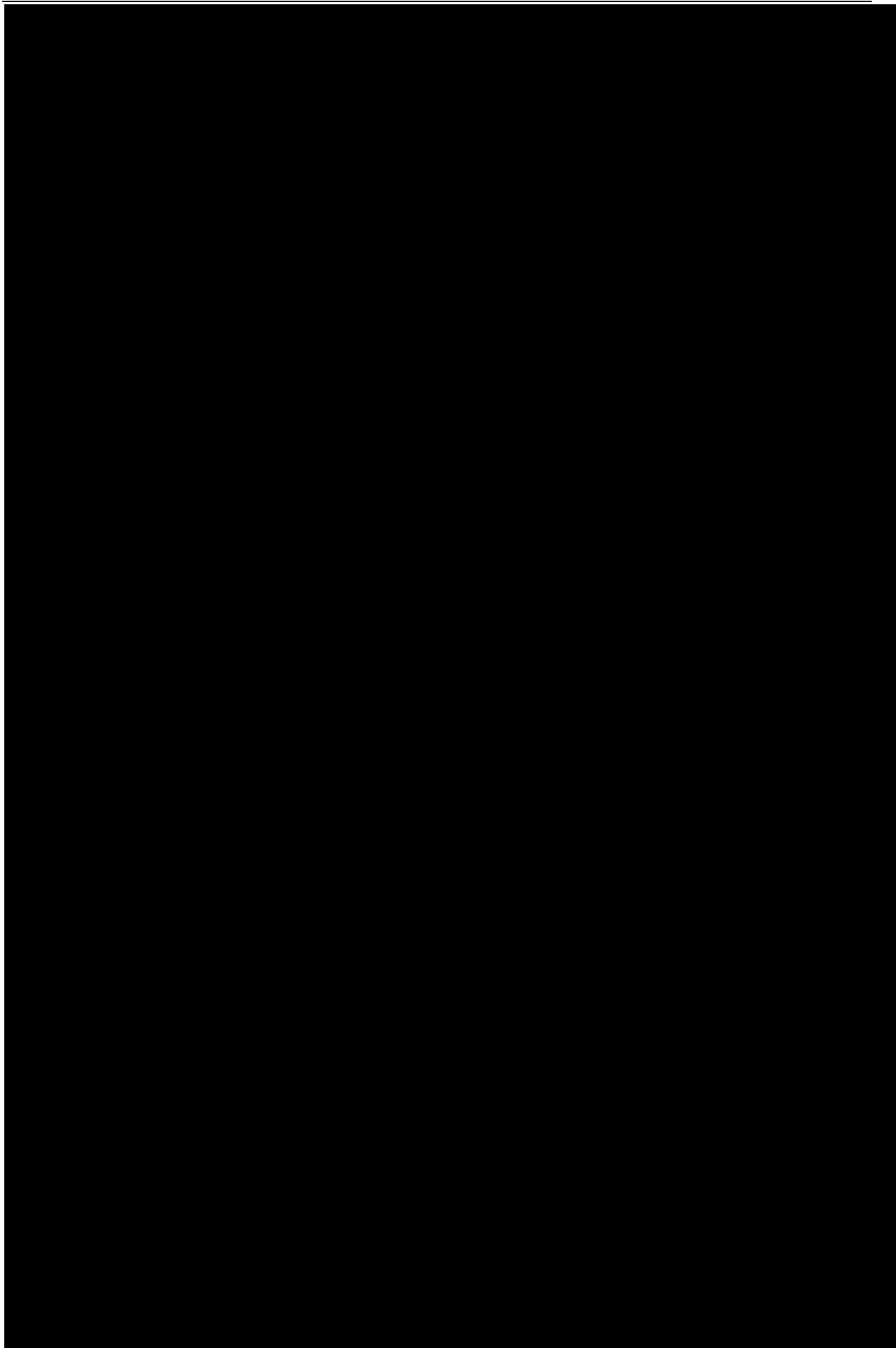


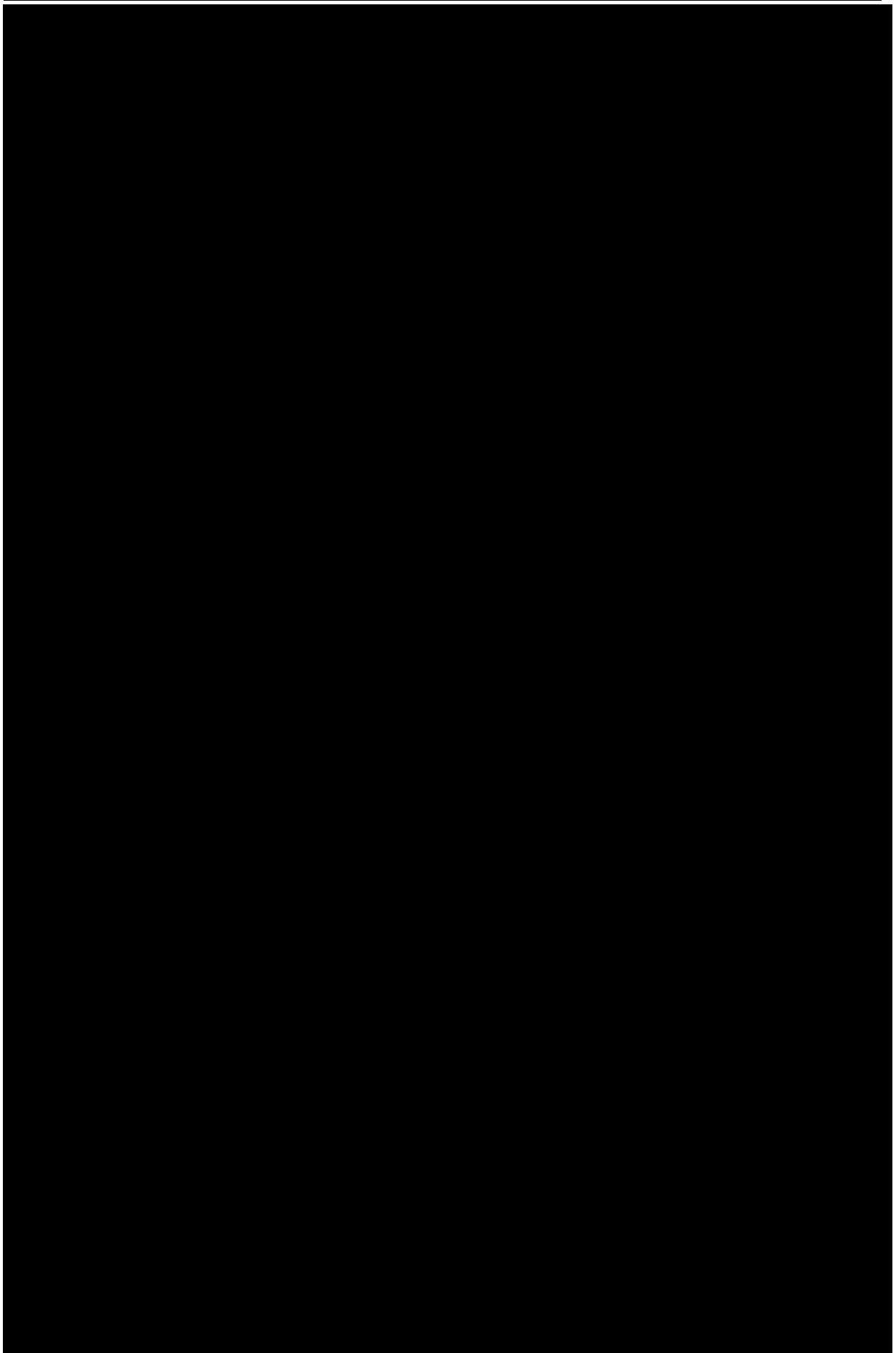


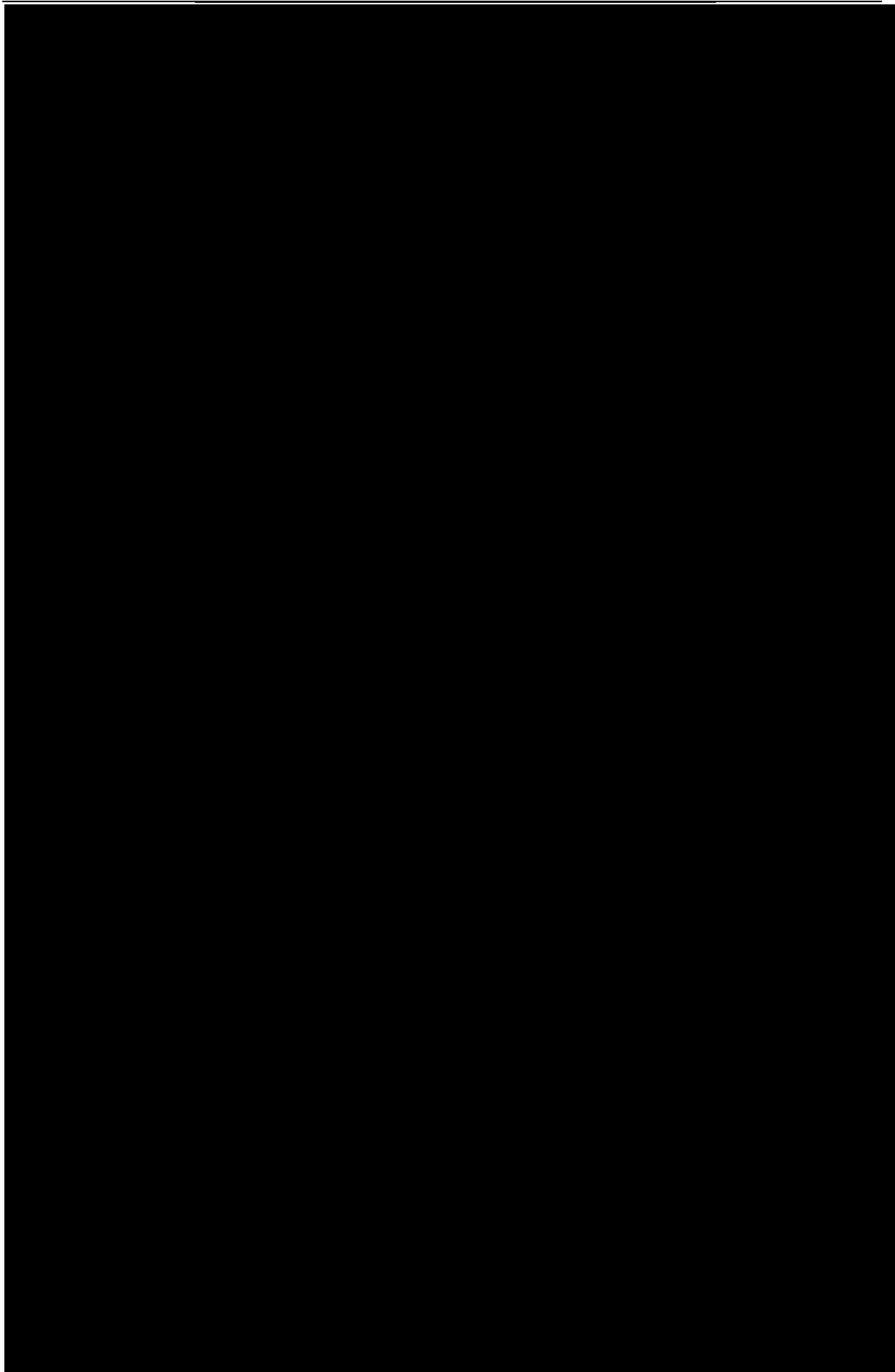
THIS PAGE IS INTENTIONALLY LEFT BLANK

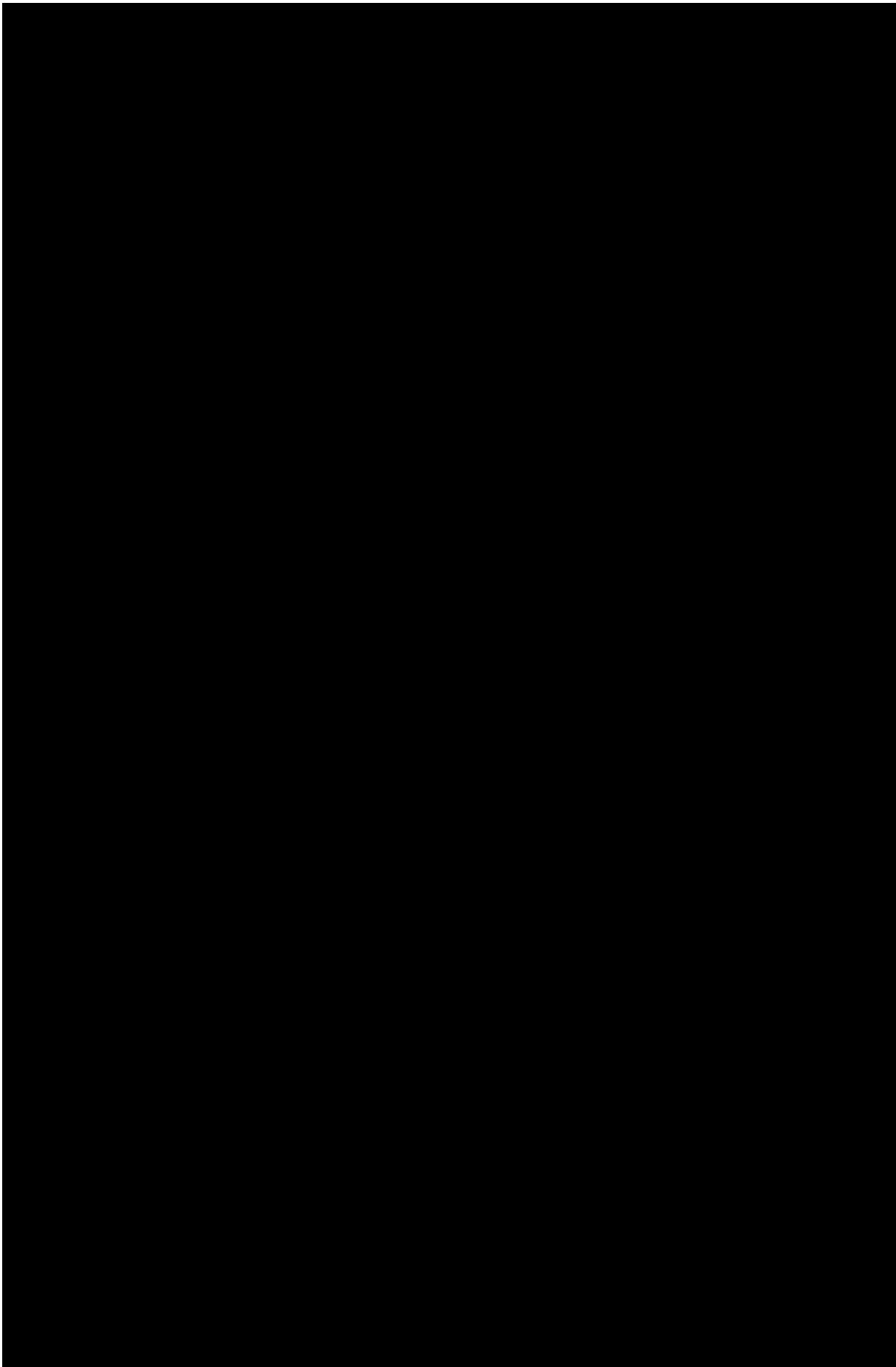
**SCHEDULE 2-3**

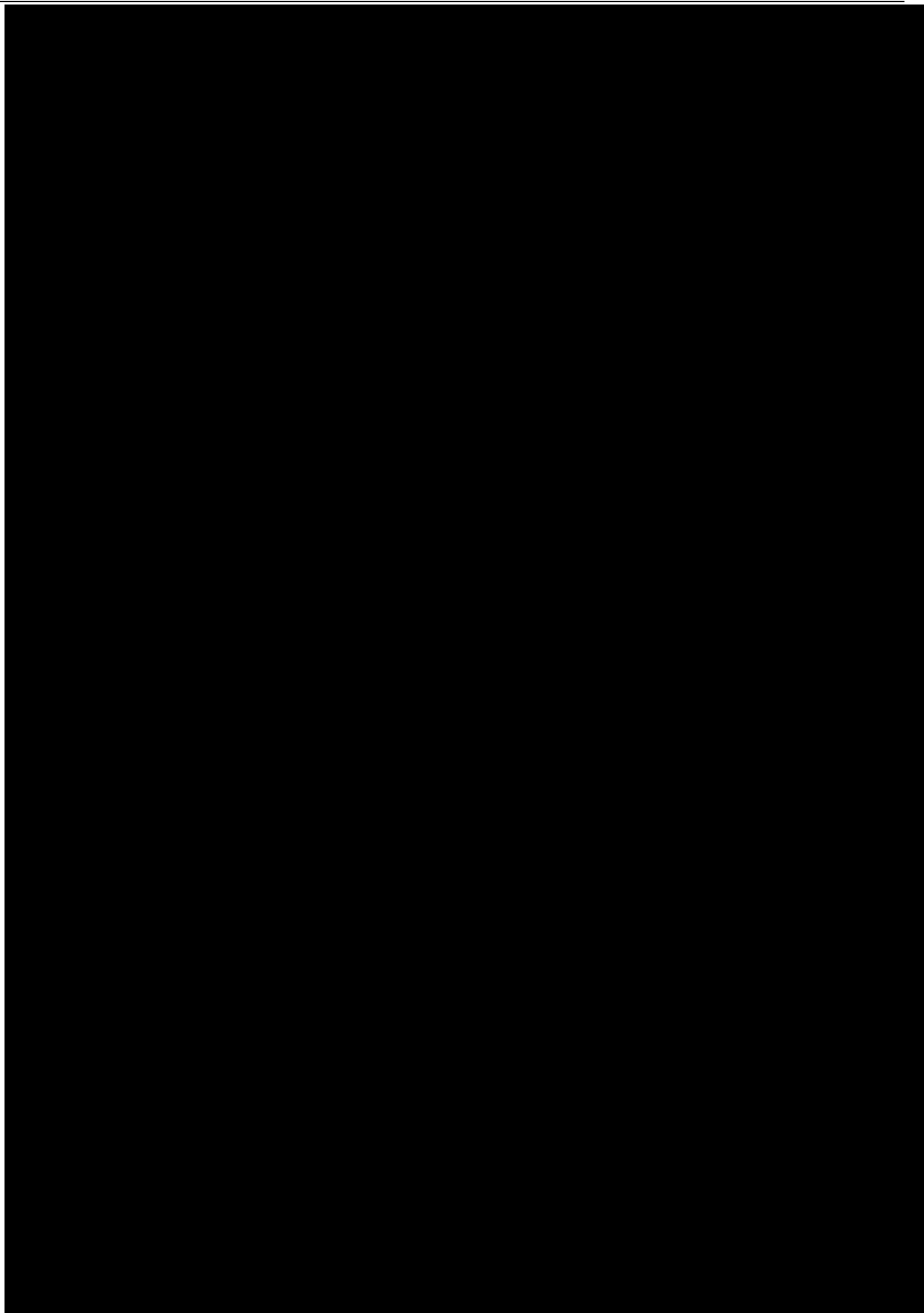


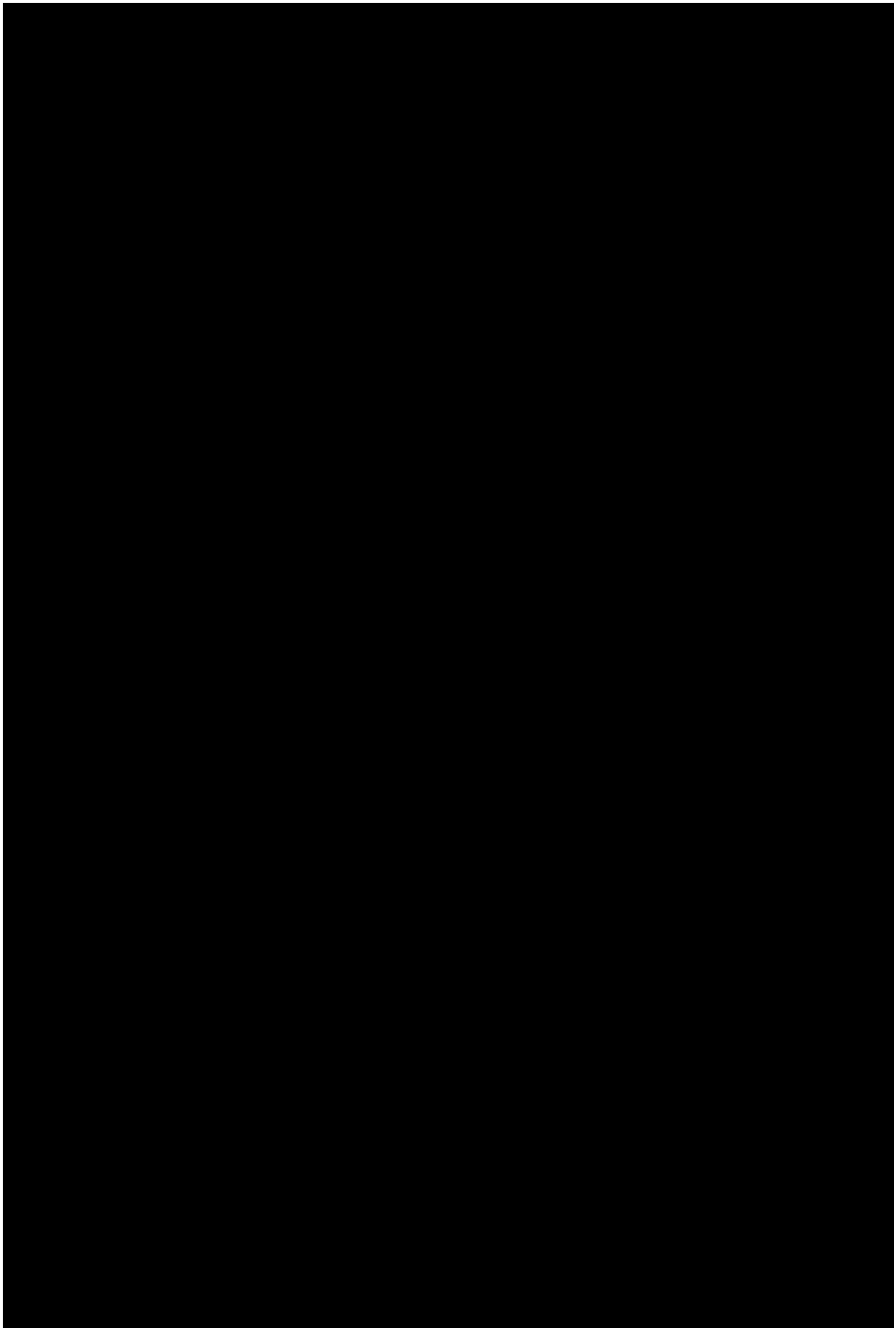


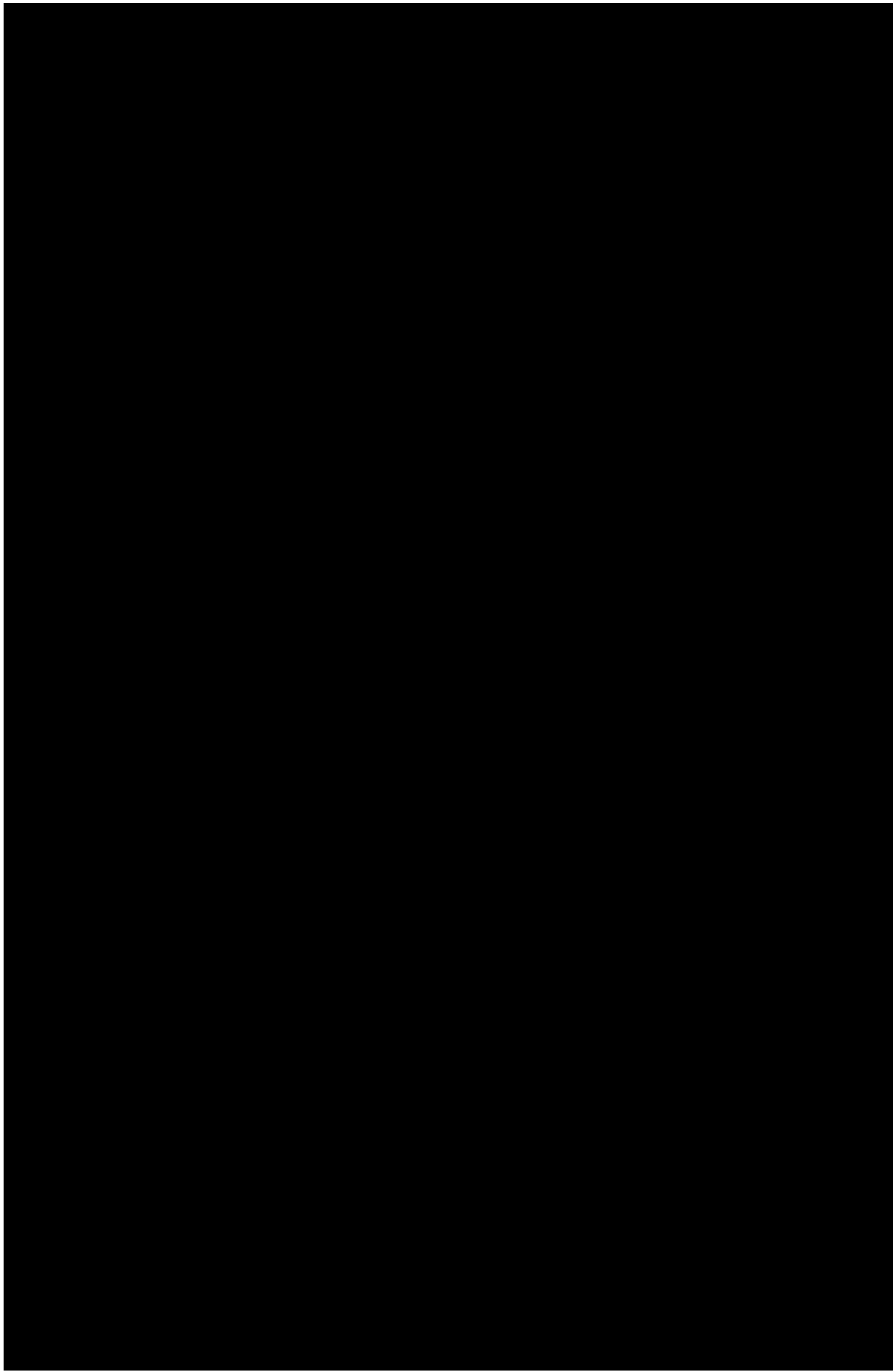


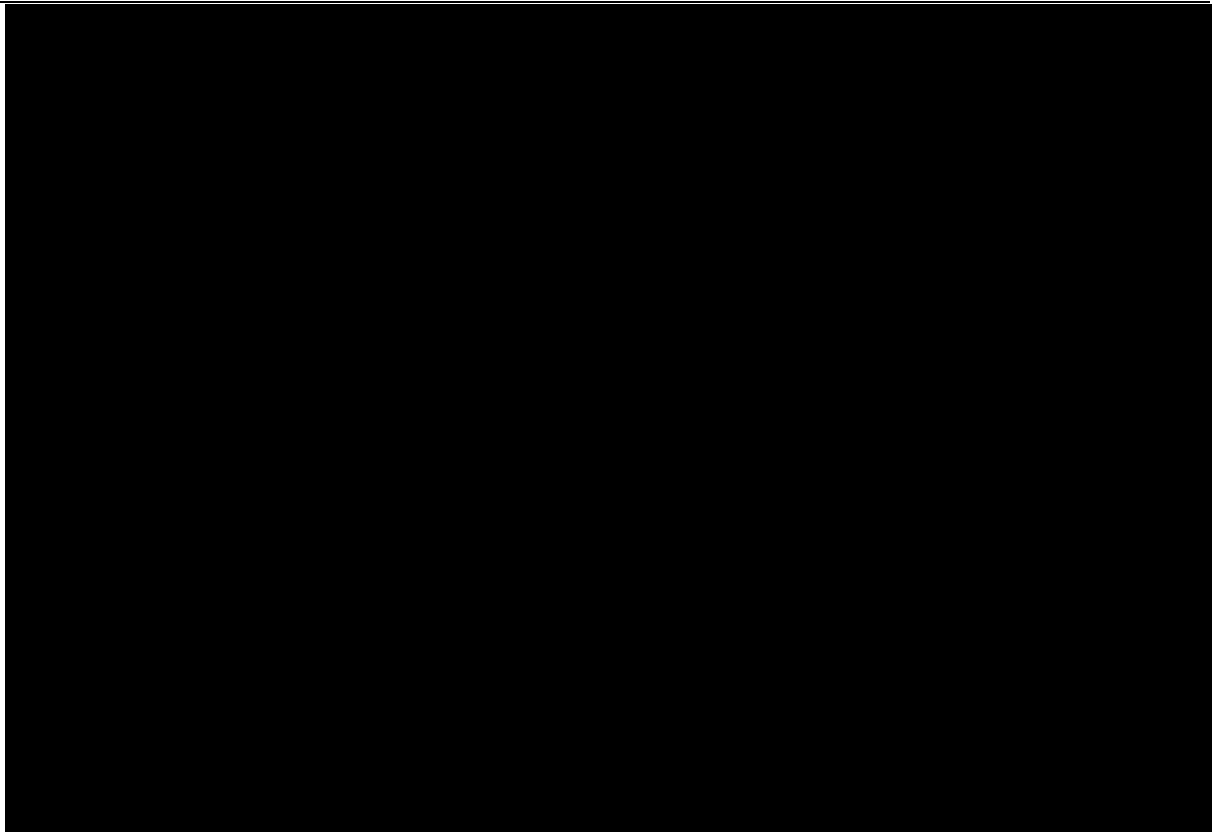












THIS PAGE IS INTENTIONALLY LEFT BLANK

---

**SCHEDULE 2-4**

**INVOICING PROCEDURE**

**1. INTRODUCTION**

1.1. This Schedule 2-4 sets out the Invoicing Procedure that shall apply to this Contract.

**2. INVOICING PROCEDURE**

2.1. submit invoices in accordance with the Service Acceptance Procedures (Schedule 2-5) directly to:

For the Attention of: The Financial Controller The Security Industry Authority  
PO Box 49768  
LONDON WC1V 6WY

2.2. Invoices shall specify:

- 2.2.1. the unique Order reference 1377-
- 2.2.2. the Invoice number (accounting reference number);
- 2.2.3. [the payment milestone (if any) within this Contract to which the invoice relates and a summary of the corresponding Ordered Services;]
- 2.2.4. the Monthly Unit based charge and the breakdown i.e. number of units and Charge per LDRM that is applied;
- 2.2.5. the pass through charges and supporting documentation detailing the unit price and volumes;
- 2.2.6. Change control Charges together with signed acceptance form to show the changes accepted by the CUSTOMER and the unique order number issued by the CUSTOMER to authorise the change request;
- 2.2.7. any Service Credits due;
- 2.2.8. the line value;
- 2.2.9. total value excluding Value Added Tax (VAT);
- 2.2.10. the VAT percentage
- 2.2.11. the total value including VAT; and
- 2.2.12. the tax point date relating to the rate of VAT shown.

**3. INVOICE PAYMENT**

3.1. The CUSTOMER shall pay all valid invoices submitted in accordance with the provisions of this Schedule 2-4 in accordance with the provisions of Clause 5.

3.2. In the event of a disputed invoice, the CUSTOMER shall make payment in respect of any undisputed amount in accordance with the provisions of Clause 5 and return the invoice to the CONTRACTOR within ten (10) Working Days of receipt with a covering statement proposing amendments to the invoice and/or the reason for any non-payment. The CONTRACTOR shall respond within ten (10) Working Days of receipt of the returned invoice stating whether or not the CONTRACTOR accepts the CUSTOMER's proposed amendments. If it does, then the CONTRACTOR shall supply with the response a replacement valid invoice. If it does not, then the matter shall be dealt with in accordance with the provisions of Clause 18.

**4. PAYMENT PROFILE**

4.1. The Payment Profile in respect of the Ordered Goods and Ordered Services is as follows:

4.1.1. As per the charges in section 2 of Schedule 2-3;

4.1.2. Monthly in arrears.

4.1.3. In accordance with the payment process as set out in document LDL/SIA/INVPRO1 version 0.3.

**SCHEDULE 2-5**

**ACCEPTANCE PROCEDURES**

**1. INTRODUCTION**

- 1.1. This Schedule 2-5 specifies the Acceptance Procedures and the Acceptance Test Criteria to be used in the acceptance of the new or additional Ordered Goods and new or additional Ordered Services.

**2. ACCEPTANCE PROCEDURES**

- 2.1. The CONTRACTOR shall, during the Acceptance Test Period, make available the Ordered Goods and Ordered Services to the CUSTOMER for the Acceptance Procedures to be performed.
- 2.2. The CUSTOMER will conduct Acceptance Tests on the Ordered Goods and Ordered Services to test whether they meet the requirement specified in the Order and meet the appropriate Service Levels.
- 2.3. The CUSTOMER may perform the Acceptance Procedures in respect of the Ordered Goods and Ordered Services.
- 2.4. The Acceptance Procedures shall be recorded as successful and the CONTRACTOR notified accordingly where all the Acceptance Test Criteria are met.
- 2.5. The Acceptance Procedures shall be recorded as unsuccessful and the CONTRACTOR notified accordingly where any of the Acceptance Test Criteria are not met.
- 2.6. In the event that the Acceptance Procedures in respect of Ordered Goods or Ordered Services or any part thereof, have not been recorded as successful pursuant to paragraph 2.4 by the end of the relevant Acceptance Test Period, the CUSTOMER will extend the Acceptance Test Period by a period of ten (10) Working Days (or such other period as the parties may agree) during which the CONTRACTOR shall correct the faults which caused the Acceptance Procedures to be recorded as unsuccessful and the Acceptance Procedures shall be re-performed.
- 2.7. In the event that after the CUSTOMER has extended the Acceptance Test Period pursuant to paragraph 2.6 the relevant Acceptance Procedures have not been recorded as successful by the end of that period, the CUSTOMER shall, without prejudice to its other rights and remedies, be entitled to:
- 2.7.1. extend the Acceptance Test Period for a further period (or periods) specified by the CUSTOMER during which the CONTRACTOR shall correct the faults which caused the Acceptance Procedures to be recorded as unsuccessful and the Acceptance Procedures shall be re-performed; or
- 2.7.2. reject the Ordered Goods and Ordered Services and terminate this Contract and receive a full refund of all sums paid under this Contract in respect of the supply of the Goods and the provision of the Ordered Services.
- 2.8. If the CUSTOMER fails to carry out the relevant Acceptance Tests within the Acceptance Test Period and such failure is wholly and solely due to the actions or inactivity of the CUSTOMER, the Acceptance Tests shall be deemed to have been completed successfully.

**3. ACCEPTANCE TEST CRITERIA**

## ICT GOODS AND ASSOCIATED SERVICES

---

- 3.1. The Acceptance Test Criteria pertaining to items of new and additional Ordered Goods and new and additional Ordered Services, as specified in the Contract Change Note
- 3.2. The Ordered Goods and Ordered Services being transferred on the Service Commencement Date shall be deemed to have been accepted one month after Service Commencement Date unless the CUSTOMER can demonstrate an Incident or show the Service Levels are below those agreed in Schedule 2-2. Any acceptance test criteria will be agreed between the parties under the Service Transfer Plan for the service being transferred from the Existing Contract.

**SCHEDULE 2-6**

**CONTRACT & SERVICE MANAGEMENT**

**1. INTRODUCTION**

- 1.1 This Schedule 2-6 specifies the requirements in respect of Contract management issues.

**2. CONTRACT MANAGEMENT STRATEGY**

- 2.1 The CONTRACTOR shall provide a Contract Manager for the term of the Agreement and any handover period.
- 2.2 The CONTRACTOR'S Contract Manager shall develop a Contract Management Strategy.
- 2.3 The Contract Management Strategy shall outline how the CONTRACTOR will manage:
- 2.3.1 Change;
  - 2.3.2 The Service Transfer Plan deliverables
  - 2.3.3 Service management and service measurements
  - 2.3.4 Contract deliverables and compliance
  - 2.3.5 Relationships, including between CUSTOMER and CONTRACTOR staff, sub contractors and any other third parties; and
  - 2.3.6 Quality of data.
- 2.4 The CONTRACTOR shall, within one (1) month of the commencement of the Contract, deliver to the CUSTOMER the Contract Management Strategy for approval.
- 2.5 The CUSTOMER shall review the Contract Management Strategy within fourteen (14) working days of receipt from the CONTRACTOR and shall notify the CONTRACTOR of any reasonable amendments or revisions required.
- 2.6 The CONTRACTOR shall within ten (10) working days of being notified of the amendments or revisions by the CUSTOMER, amend or revise the Contract Management Strategy in accordance with the CUSTOMER'S reasonable requests and shall deliver to the CUSTOMER the revised version for approval.
- 2.7 The CUSTOMER shall, at the request of the CONTRACTOR provide reasonable co-operation and assistance to enable the CONTRACTOR to perform its obligations under this clause 2.

**3. REPORTS**

- 3.1 When requested by the CUSTOMER, the CONTRACTOR shall provide Reports electronically to the CUSTOMER's Contract Manager.
- 3.2 The CUSTOMER may request, in writing, exceptional Reports on exceptional items or issues.
- 3.3 Such exceptional Reports, shall be submitted within ten (10) working days from the request.

3.4 The CONTRACTOR shall submit monthly Reports by the 5<sup>th</sup> day of the following month.

3.5 Monthly Reports shall include:

- 3.5.1 a record of the Ordered Goods supplied to the CUSTOMER;
- 3.5.2 a record of the Ordered Services provided to the CUSTOMER;
- 3.5.3 a record of the invoices raised by the CONTRACTOR;
- 3.5.4 details of Sub-Contractors used;
- 3.5.5 a record of any failures to supply Ordered Goods or provide Ordered Services in accordance with this Contract including Contract non-conformance and security breach;
- 3.5.6 details of the number and nature of complaints from the CUSTOMER.
- 3.5.7 Service management reports that measure performance against Service Level targets e.g. Operation and Customer Review and SLA report including:
  - 3.5.7.1 performance;
  - 3.5.7.2 non-conformance;
  - 3.5.7.3 service credits incurred;
  - 3.5.7.4 current & trend information (KPIs);
- 3.5.8 Performance reporting following major events, including major Incidents and changes;
- 3.5.9 Resolution of performance issues;
- 3.5.10 Monthly and Cumulative Contract costings
- 3.5.11 Gain share;
- 3.5.12 A system workload performance report including volume and resource utilisation;
- 3.5.13 The number of Applications at each stage of the process, including Gross Applications, Net Applications and LDRM's.
- 3.5.14 A monthly Quality of Service report providing details and analysis of operational and contractual performance
- 3.5.15 Service satisfaction analysis carried out for users of the services and the Applicants including monthly quality of service (QOS) report (CONTRACTOR management information system (MIS) report shared with the CUSTOMER)
- 3.5.16 Service improvement plans;
- 3.5.17 Agreed change controls e.g. change programme review – programme board summary, system upgrade and change requests;
- 3.5.18 record of risks identified by the CONTRACTOR to the CUSTOMER, including any risks identified through the CONTRACTOR's Data Quality Policy and the risk register;
- 3.5.19 Security review and accreditation;
- 3.5.20 Strategic development and progress updates; and

3.5.21 Other contract and service management reporting to be agreed with the CUSTOMER Contract Manager which shall be provided without additional cost to the CUSTOMER.

3.6 The Reports and data contained therein, shall be submitted in accordance with the quality standards as set out in the Contract Management Strategy.

3.7 The reports will be produced to meet a specified reporting schedule timing and format to be set out in the Contract Management Strategy.

#### **4. REVIEW MEETINGS**

4.1 When requested by the CUSTOMER, the CUSTOMER contract manager and CONTRACTOR's contract manager and/or nominated representatives shall attend review meetings at a location and frequency to be agreed between the CUSTOMER contract manager and CONTRACTOR's contract manager

4.2 The CONTRACTOR shall attend service reviews with the CUSTOMER to discuss any changes to the service scope, Service Levels, contract or the business needs on a regular basis to be agreed with the CUSTOMER.

4.3 Service review meetings are to be held monthly unless otherwise agreed.

4.4 Information security shall be a standing agenda item for the review meetings.

4.5 The outputs of the review meeting are:

4.5.1 Report on Service Performance with commentary by CUSTOMER or CONTRACTOR or both;

4.5.2 Service Credits applicable as a result of Service Performance;

4.5.3 Service Improvement Plan requirements;

4.5.4 Agreed Change Controls;

4.5.5 Subsequent Actions from the Review Meeting agreed between the CONTRACTOR and the CUSTOMER.

4.5.6 Project plan outlining how the risks identified by the CONTRACTOR and/or the CUSTOMER are to be mitigated.

4.5.7 Report on the progress of outstanding actions or completed actions from previous Review Meetings.

4.6 The CONTRACTOR shall:

4.6.1 hold interim meetings at agreed intervals to discuss performance, achievements, issues and action plans involving appropriate Stakeholders.

4.6.2 ensure that any proposed changes to contract(s), and Service Levels from these meetings are documented.

4.6.3 ensure that any proposed changes to contract(s), and Service Levels from these meetings enter the CUSTOMER Change Management process as appropriate.

#### **5. KEY PERSONNEL**

5.1 The CONTRACTOR's Key Personnel nominated to fulfil the roles in the CONTRACTOR's Management Organisation, other CONTRACTOR's Key Personnel who shall have direct involvement with the CUSTOMER, shall be as specified in this schedule (2.6) and individuals listed for each role at Appendix Two.

5.2 The CONTRACTOR shall not replace an individual identified as a member of the CONTRACTOR's Key Personnel from the date of this Agreement until the expiry of a period of 12 Months from the Commencement Date without the written agreement of the CUSTOMER, which shall not be unreasonably withheld or delayed.

5.3 Where the CONTRACTOR wishes to replace a member of the CONTRACTOR Key Personnel or a new key post has been identified by the CUSTOMER then the CONTRACTOR shall provide to the CUSTOMER the curriculum vitae of the proposed new member of the CONTRACTOR Key Personnel. The CUSTOMER may interview any such proposed new member of the CONTRACTOR Key Personnel. The CONTRACTOR shall take into account any reasonable request by the CUSTOMER to change the proposed new member of the CONTRACTOR's Key Personnel following such interview.

5.4 The CONTRACTOR shall not replace an individual identified as a member of the CONTRACTOR's Key Personnel from the date of this Agreement until the expiry of a period of 12 Months from the Commencement Date without the written agreement of the CUSTOMER, which shall not be unreasonably withheld or delayed.

## **6. MANAGE SERVICE DELIVERY**

6.1 The CONTRACTOR shall manage the Ordered Goods and Ordered Services provided to the CUSTOMER.

6.2 The CONTRACTOR shall:

- 6.2.1 adhere to ITIL best practice.
- 6.2.2 be certified in ISO/IEC 20000.
- 6.2.3 ensure that all personnel involved in the provision of service management are suitably skilled to perform effectively.
- 6.2.4 ensure that the skill set of all personnel involved in the provision of service management is reviewed on a frequency to be agreed with the CUSTOMER.
- 6.2.5 agree with the CUSTOMER a formal complaints process to manage complaints regarding the managed service provision.
- 6.2.6 record all formal complaints against the CUSTOMER and ensure they are investigated, acted upon, reported and formally closed. Where a complaint is not resolved through the normal channels, it should be escalated to the CUSTOMER's Contract Manager.
- 6.2.7 have a named individual or individuals who will manage the contract and business relationship with CUSTOMER.
- 6.2.8 develop and maintain a risk register relating to the services provided compliance with the CUSTOMER Risk Management Framework.
- 6.2.9 be responsible for maintaining inventory control of all stock items required to manage the services provided.

## **7. BUSINESS IMPROVEMENT**

7.1 Both the CONTRACTOR and the CUSTOMER shall provide representatives to attend the Business Improvement Group to discuss improvements to the managed service Solution provision.

- 7.2 Business Improvement Group terms of reference, location and meeting frequency will be agreed by both CONTRACTOR and CUSTOMER prior to commencement of this Contract.

## **8. VIRTUAL LIBRARY SERVICES**

- 8.1 The CONTRACTOR shall, prior to the Commencement Date, create a Virtual Library and shall maintain the Virtual Library throughout the Term.

- 8.2 The CONTRACTOR shall ensure that the Virtual Library is:

- 8.2.1 capable of holding, and allowing access to, the information referred to in paragraph 8.3 below;
- 8.2.2 accessible to such nominated CUSTOMER staff as agreed between the parties; and
- 8.2.3 password protected to ensure that it cannot be viewed by third parties.

- 8.3 The CONTRACTOR shall throughout the term, without charge to the CUSTOMER, store in the Virtual Library, and keep up to date at all times, the following information: -

- 8.3.1 all “employee liability information” (as defined in Regulation 11 of the Transfer of Undertakings (Protection of Employment Regulations) 2006 (“the Regulations”) regarding the Contractor’s employees and its Sub-Contractors’ employees and all other persons that are from time to time engaged in the supply of the Ordered Goods or the provision of the Ordered Services and who are assigned to an organised grouping of resources or employees that would be the subject of a relevant transfer (as that term is defined in the Regulations) were the supply of the Ordered Goods or the provision of the Ordered Services be subject to a service provision change (as that term is defined in the Regulations) at that time;
- 8.3.2 all equivalent information as that referred to in paragraph 1.3.1 above in relation to all the CONTRACTOR’s employees and its sub-Contractors’ employees and all other persons that are from time to time engaged in the supply of the Ordered Goods or the provision of the Ordered Services but who would not, in the CONTRACTOR’S reasonable opinion, be subject of a relevant transfer were the supply of the Ordered Goods or the provision of the Ordered Services be subject to a service provision change (as that term is defined in the Regulations) at that time;
- 8.3.3 a register of Intellectual Property Rights used by the CONTRACTOR in the supply of the Ordered Goods or the provision of the Ordered Services, including licence terms of all third party Software;
- 8.3.4 inventory control records;
- 8.3.5 the Contract (including the schedules) together with any agreed variations to the Contract and , Change Control Notes and a change control register;
- 8.3.6 documents that the CONTRACTOR is required to produce under the Contract (including, without limitation, insurance certificates, management reports and minutes of meetings);
- 8.3.7 copies of all invoices submitted by the CONTRACTOR to the CUSTOMER pursuant to this Contract together with a summary of the monthly amounts billed by the CONTRACTOR;

- 8.3.8 the current Service Transfer Plan;
  - 8.3.9 all relevant ICT technical specifications, drawings, and user manuals;
  - 8.3.10 third party supply contracts (other than the contract with the sub-Contractor listed in Schedule 2-8) entered into by the CUSTOMER solely or primarily for the purpose of the contract together with a register of such contracts and the CUSTOMER's respective price lists;
  - 8.3.11 the current security procedures and any security plan agreed under Schedule 2-13;
  - 8.3.12 a risk register;
  - 8.3.13 list of reports from SEIBEL and all other such systems, used in the provision of the Ordered Goods and Ordered Services; and
  - 8.3.14 any other information related to the delivery of the Ordered Goods and Ordered Services as reasonably requested by the CUSTOMER.
- 8.4 The CONTRACTOR and the CUSTOMER shall, by 31<sup>st</sup> March 2010, develop protocols relating to the content, use and maintenance of the virtual library including (without limitation) protocols to ensure that the Virtual Library is used in way consistent with the parties obligations under the Data Protection Act 1998 and any applicable provisions of Schedule 2-13.
- 8.5 The CUSTOMER shall at any time during the Term have the right, free of charge, to view, download, copy, and use for any purpose connected with the Contract or the retendering of the contract for the supply of the Ordered Goods or the provision of the Ordered Services, any information currently stored on the Virtual Library.
- 8.6 The CONTRACTOR warrants that all information stored in the Virtual Library shall be at all times, so far as is reasonably practicable, accurate and up to date.

**SCHEDULE 2-7**

**CONTRACT CHANGE PROCEDURE**

**1. INTRODUCTION**

- 1.1 This Schedule 2-7 sets out the Contract Change Procedure to be used by the CUSTOMER and the CONTRACTOR to effect changes to this Contract.

**2. PRINCIPLES**

- 2.1 The CUSTOMER and the CONTRACTOR shall conduct discussions relating to proposed changes to this Contract in good faith. Neither party shall unreasonably withhold or delay consent to the other party's proposed changes.
- 2.2 Until such time as a Contract Change Note (CCN) has been signed by both parties, the CONTRACTOR shall continue to supply and make available to the CUSTOMER the Ordered Goods and Ordered Services in accordance with this Contract.
- 2.3 Any work undertaken in connection with any proposed change to this Contract by the CONTRACTOR, its Sub-Contractors or agents (other than that which has previously been agreed in accordance with the provisions of paragraph 2.2 of this Schedule 2-7) shall be undertaken entirely at the expense and liability of the CONTRACTOR unless otherwise agreed between the CUSTOMER and the CONTRACTOR in advance.
- 2.4 Any discussions, negotiations or other communications which may take place between the parties in connection with any proposed change to this Contract, including but not limited to the submission of any written communications, prior to the signing by both parties of the relevant CCN, shall be without prejudice to the rights of either party.

**3. PROCEDURE**

- 3.1 Should either party wish to amend this Contract, that party shall submit a draft CCN detailing the proposed change to the other party using the pro forma at paragraph 7 of this Schedule 2-7 in accordance with Clause 9 and the CUSTOMER's change management process .
- 3.2 Within ten (10) Working Days of the submission of a draft CCN (or such other period as may be agreed between the parties) the receiving party shall respond to the draft CCN in accordance with Clause 9. If appropriate, the parties shall enter into discussions to discuss the draft CCN.
- 3.3 Discussion between the parties following the submission of a draft CCN shall result in either:
- 3.3.1 agreement between the parties on the changes to be made to this Contract (including agreement on the date upon which the changes are to take effect (the "effective date")), such agreement to be expressed in the form of proposed revisions to the text of the relevant parts of this Contract; or
- 3.3.2 no further action being taken on that draft CCN.
- 3.4 A draft CCN, the content of which has been agreed between the parties in accordance with paragraph 3.3.1 of this Schedule 2-7, shall be uniquely identified by a sequential number allocated by the CUSTOMER.

- 3.5 Two (2) copies of each CCN shall be signed by the CONTRACTOR and submitted to the CUSTOMER not less than ten (10) Working Days prior to the effective date agreed in accordance with paragraph 3.3.1 of this Schedule 2-7.
- 3.6 Subject to the agreement reached in accordance with paragraph 3.3.1 of this Schedule 2-7 remaining valid, the CUSTOMER shall sign both copies of the approved CCN within five (5) Working Days of receipt by the CUSTOMER. Following signature by the CUSTOMER, one (1) copy of the signed CCN shall be returned to the CONTRACTOR by the CUSTOMER.
- 3.7 A CCN signed by both parties shall constitute an amendment to this Contract pursuant to Clause 8.

#### **4. IMPLEMENTATION OF CHANGE.**

4.1 The CONTRACTOR shall:

- 4.1.1 ensure that all changes to the Solution are carried out in a planned and authorised manner in accordance with the SIA change management process.
- 4.1.2 ensure that a Change Control Note is completed where the Solution is to change.
- 4.1.3 ensure that a Change Control Note includes, but is not limited to: change description, justification, impact summary, Configuration Items impacted, critical success factors, assumptions, constraints, risks, business areas affected & approval.
- 4.1.4 agree the tests and outcomes that will be required for all Change Control Notes with the CUSTOMER.
- 4.1.5 assess the impact and risk of each Change Control Note. This shall be prioritised and approved by the CUSTOMER.
- 4.1.6 schedule the implementation of approved Change Control Note in agreement with the CUSTOMER.
- 4.1.7 implement revisions to all documentation relating to Change Control Note so that these remain in line with all services changed.
- 4.1.8 ensure service and infrastructure changes have a clearly defined and documented scope.
- 4.1.9 ensure the change management process includes a process to rollback or remedy if unsuccessful without impacting the CUSTOMER business operation.
- 4.1.10 ensure the changes are approved, implemented and reviewed in accordance with the CUSTOMER's change management process.
- 4.1.11 follow the CUSTOMER's change management process to authorise and implement emergency changes.
- 4.1.12 ensure a schedule containing details of all the changes approved and their proposed implementation dates is maintained and communicated to relevant parties.
- 4.1.13 ensure the scheduled implementation dates for changes is used as the basis for definition of the change and release schedule.

- 4.1.14 perform change analysis, recording results and conclusions drawn in accordance with the agreed success criteria.
- 4.1.15 ensure change includes but is not limited to: detecting increasing levels of changes, frequently recurring types, emerging trends and other relevant information.
- 4.1.16 ensure that actions for improvement identified from the CUSTOMER's change management process shall be recorded and input into a plan for improving the service.
- 4.1.17 provide an impact assessment in response to each request for change within n days of receipt, in accordance with the agreed service level.
- 4.1.18 take part in consultation meetings with the CUSTOMER, to discuss potential changes to the Solution on a frequency to be agreed with the CUSTOMER.
- 4.1.19 report on business improvement outcomes of changes implemented for the managed service and Solution, in a format to be agreed with the CUSTOMER.

## **5. MANAGE SERVICE RELEASE**

### **5.1 The CONTRACTOR shall:**

- 5.1.1 be responsible for the controlled release of changes to the Solution following approval from the CUSTOMER.
- 5.1.2 be responsible for the release management of all changes to Configuration Items under its control, ensuring that versions are installed in appropriate locations and enhancements made to software are released in a controlled manner following approval from the CUSTOMER.
- 5.1.3 confirm the details of a release plan in consultation with the CUSTOMER.
- 5.1.4 obtain approval from the CUSTOMER for all releases.

### **5.2 The release plan shall include as a minimum the following details:**

- 5.2.1 release definition
- 5.2.2 Configuration Items affected
- 5.2.3 Cost
- 5.2.4 implementation approach
- 5.2.5 phasing, dates
- 5.2.6 user test results
- 5.2.7 acceptance/success criteria
- 5.2.8 communications plans
- 5.2.9 training plans
- 5.2.10 acceptance test results
- 5.2.11 impact analysis and
- 5.2.12 contingency arrangements.

### **5.3 The CONTRACTOR shall:**

- 5.3.1 report progress against the release plan to the CUSTOMER on at least a monthly basis.

- 5.3.2 provide a dedicated resource to manage the release plan.
- 5.3.3 carry out the following testing activities prior to involving the CUSTOMER in user acceptance testing : system testing, functional testing, integration and interface testing, performance testing, volume testing for all new releases as appropriate, only passing the new release to user acceptance testing once these tests are successful.
- 5.3.4 provide documented evidence of testing activity including final approvals..
- 5.3.5 plan and distribute releases in phases, if required and agreed by the CUSTOMER.
- 5.3.6 provide the necessary training and documentation on new releases to ensure business readiness by agreement with the CUSTOMER.
- 5.3.7 document a release policy stating the frequency and type of releases. This policy must be agreed with the CUSTOMER.
- 5.3.8 plan with the CUSTOMER the release of services, systems, software and hardware. Plans on how to roll out the release shall be agreed and authorised by the relevant CUSTOMER release authority board.
- 5.3.9 ensure the release process includes the manner in which the release shall be rolled back or remedied if unsuccessful.
- 5.3.10 ensure that release plans record the release dates and deliverables, including reference to related Contract Change Note, known errors and Problems.
- 5.3.11 ensure the release management process passes relevant information via the Incident management process to SIA Information Communication Technology Team.
- 5.3.12 assess approved requests for change for their impact on release plans.
- 5.3.13 ensure release management procedures include the updating and changing of configuration information and change records.
- 5.3.14 ensure emergency releases are managed according to a defined process that interfaces to the emergency Change Management process.
- 5.3.15 provide controlled test environments to build and test all releases prior to distribution as required.
- 5.3.16 provide a controlled training environment (data & systems) to facilitate training.
- 5.3.17 provide a training facility to deliver training courses as required to CUSTOMER staff.
- 5.3.18 ensure that release and distribution is designed and implemented so that the integrity of hardware and software is maintained during installation, handling, packaging and delivery.
- 5.3.19 consult with the SIA Information Communication Technology Team to ensure that the proposed managed service Solution is compatible with the CUSTOMER technical infrastructure (including networks & workstations).
- 5.3.20 provide a post release report including; an analysis of Incidents related to the release, an assessment of the impact on the CONTRACTOR and CUSTOMER, lessons learned and actions taken to improve release management.

5.3.21 agree with the CUSTOMER the success criteria for each release.

5.3.22 re-test the Availability Plan at every major change to the business environment.

**6. CHANGE CONTROL CHARGES**

6.1 These shall be charged when the Ordered Goods and Ordered Services implemented under the Contract Change Note is accepted by the CUSTOMER

6.2 Day rates in relation to changes to the Monthly Charge shall be charged at the rates for the man day based charges shown in Schedule 2-3 at Table 4.

**7. The CCN pro forma is as follows:**

Contract Change Note for the Contract Change Procedure

In line with the contract change procedure at schedule 2-7 of the contract dated (insert date), we request a detailed assessment of the impact of implementing the changes outlined in part one of this form. Where signed by both parties this document will become the Contract Change Notice affecting the contract for Ordered Goods and Ordered Services as specified.

In completing this form, please use the accompanying guidance notes.

<b>Change Request Title:</b>	
<b>Originator:</b>	
<b>Business Unit:</b>	
<b>Expression of Interest (EOI) Approval Date (DD/MM/YYYY):</b>	
<b>Change Request Approval Date (DD/MM/YYYY):</b>	
<b>SIA Control No.: (To be entered by Contract Manager)</b>	

**1. Requestor Information**

***Proposed Change Description***

**Description / Problem / Purpose**

*(The current business problem being addressed - essential to know where the business is moving away from - ensure you detail root problem not just the symptoms)*

**Justification, objective and expected benefits  
(Please refer to Strategic Prioritisation Framework for guidance):**

**Date required:**

**Strategic Prioritisation Score**

**IMPACT ASSESSMENT:**

**2. Impact Summary**

## ICT GOODS AND ASSOCIATED SERVICES

### 2. Impact Summary

<b>Configuration Items Affected</b> (e.g. product specifications):					
<b>Detailed Impact Analysis Required?</b> <i>(check one)</i>	<b>Yes</b> [   ]	<b>No</b> [   ] If No, please give reason here			
<b>Impact on Development Resource:</b>					
<b>Impact on Ongoing Service Resource:</b>					
<b>Impact on Cost:</b>	Please detail below				
<b>Additional Software / Hardware Requirements:</b>	<i>Annual charges (£)</i>	<i>One-Off (£)</i>	<i>Equipment (£)</i>	<b>Total Cost (£)</b>	<b>Price to SIA (£)</b>
<b>Additional Resource Requirements:</b>	<i>Work Days (give details and no. of work days)</i>			<b>Total Cost (£)</b>	<b>Price to SIA if applicable (£)</b>
<b>Total Impact on Cost:</b>					

### 3. Change Definition / Scope:

#### Primary Products

Description of products / deliverables that define the change. The change will be complete when all products are in place.

<b>P1</b>	
<b>P2</b>	
<b>P3</b>	
<b>P4</b>	

#### Critical Success Factors (CSF)

Specific items that must be in place for the change to succeed. These tend to be behavioural/organisational factors.

<b>CSF1</b>	
<b>CSF2</b>	
<b>CSF3</b>	

## ICT GOODS AND ASSOCIATED SERVICES

### Critical Success Factors (CSF)

Specific items that must be in place for the change to succeed. These tend to be behavioural/organisational factors.

<b>CSF4</b>	
-------------	--

### Key Milestones (To be completed by Development Team)

Key milestones, detailed milestones can be added as they are known.

<b>Start Date</b>	
-------------------	--

<b>End Planning</b>	
---------------------	--

<b>End Project</b>	
--------------------	--

### Assumptions

Specific assumptions that you may hold to enable the change to succeed.

<b>A1</b>	
-----------	--

<b>A2</b>	
-----------	--

<b>A3</b>	
-----------	--

### Constraints

A condition imposed on the project which may impact on the success of the change and may influence planning. An owner may be set against each constraint to provide mitigation.

	Owner
--	-------

<b>C1</b>		
-----------	--	--

<b>C2</b>		
-----------	--	--

<b>C3</b>		
-----------	--	--

### Risks

A potential future event that, if it happens, will have a negative impact on the change. Refer to organisational risk scoring matrix to quantify likelihood of occurrence and impact.

	L'hood	Impact
--	--------	--------

<b>R1</b>			
-----------	--	--	--

<b>R2</b>			
-----------	--	--	--

<b>R3</b>			
-----------	--	--	--

### Affected Areas

<b>Contact Centre</b>	<input type="checkbox"/>	<b>DHC</b>	<input type="checkbox"/>	<b>Licensing</b>	<input type="checkbox"/>
-----------------------	--------------------------	------------	--------------------------	------------------	--------------------------

## ICT GOODS AND ASSOCIATED SERVICES

Affected Areas					
ICT Infrastructure	<input type="checkbox"/>	Marketing	<input type="checkbox"/>	Intelligence	<input type="checkbox"/>
Other – please state	<input type="checkbox"/>				

<b>4. Approval</b>			
<b>Risk associated with implementing the change:</b>			
<b>Risk associated with not implementing the change:</b>			
<b>Proposed Development Priority:</b>			
<b>RFC Sponsor sign off:</b>			
<b>CSCMG Priority:</b>			
<b>Approved:</b>	<b>Yes [ ]</b>	<b>No [ ]</b>	<b>Further information required [ ]</b>

IT IS AGREED as follows:

1. With effect from [date] the Contract shall be amended as set out below:

[Details of the amendments to the Contract to be inserted here – to include the explicit changes required to the text in order to effect the change, i.e.

Clause/Schedule/paragraph number, required deletions and insertions etc]

2. Save as herein amended, all other terms and conditions of the Contract inclusive of any previous CCNs shall remain in full force and effect.

**Signed for and on behalf of BT/LDL**

**Signature .....**

**Name .....**

**Title .....**

**Date .....**

**Signed for and on behalf of the Security Industry Authority**

**Signature.....**

**Name .....**

**Title .....**

**Date .....**

IT IS AGREED as follows:

**The Change is accepted by the SIA as delivered to the specification.**

**Signed for and on behalf of the Security Industry Authority**

**Purchase Order Number (if required).....**

**Name .....**

**Title           Authorised Acceptance Manager**

**Date .....**



**SCHEDULE 2-8**  
**SUB-CONTRACTORS**

**1. INTRODUCTION**

1.1 This Schedule 2-8 contains:

- 1.1.1 details of the Sub-Contractors to be employed by the CONTRACTOR in the supply of Ordered Goods and the provision of Ordered Services; and
- 1.1.2 the procedure to select, appoint and manage Sub-Contractors.

**2. SUB-CONTRACTORS**

2.1.1 Table of Sub-Contractors:

Name and full contact details	Obligation
Liverpool Direct Limited	Managed Service Provider for Licence Provision
<div style="background-color: black; width: 100%; height: 1.2em;"></div>	
Municipal Buildings, Dale Street	
Liverpool, L2 2DH	
Registered number: LRQ 0940000	

**3. PROCEDURE TO SELECT, APPOINT AND MANAGE SUB-CONTRACTORS**

- 3.1 Where the CONTRACTOR proposes to assign, novate, sub-contract or otherwise dispose of this Contract or any part thereof, unless otherwise agreed in writing by the CUSTOMER ( and subject to the provisions in Clause 26.2 of the Contract), the CONTRACTOR shall adopt the Contract Change Procedure at Schedule 2-7 of this Contract in relation to the proposed change.
- 3.2 Where the CUSTOMER has consented to the sub-contracting of all or part of the Ordered Goods and Ordered Services, the CONTRACTOR shall (unless the CUSTOMER's representative agrees otherwise) ensure that the contract between the CONTRACTOR and it's sub-contractor contain similar terms and conditions to those contained in the Contract as are applicable to the sub-contracted Ordered Goods and Ordered Services.
- 3.3 The CONTRACTOR shall be responsible for the errors and omissions of its sub-contractors as if they were its own.
- 3.4 The CONTRACTOR shall not use self-employed individuals in the provision of the Services without the Customer's prior written approval.



**SCHEDULE 2-9**

**DISPUTE RESOLUTION PROCEDURE**

**1. INTRODUCTION**

- 1.1 In the event that a dispute cannot be resolved by the CUSTOMER and CONTRACTOR representatives nominated under Clause 18.3 within a maximum of ten (10) Working Days after referral, the dispute shall be further referred to mediation in accordance with the provisions of Clause 18.4.
- 1.2 Subject always to the provisions of Clause 18, nothing in this dispute resolution procedure shall prevent the CUSTOMER or the CONTRACTOR from seeking from any court of the competent jurisdiction an interim order restraining the other party from doing any act or compelling the other to do any act.

**2. MEDIATION**

- 2.1 The procedure for mediation pursuant to Clause 18.5 and consequential provisions relating to mediation shall be as follows:
- 2.1.1 a neutral adviser or mediator ('the Mediator') shall be chosen by agreement between the CUSTOMER and the CONTRACTOR or, if they are unable to agree upon the identity of the Mediator within ten (10) Working Days after a request by one party to the other (provided that there remains agreement for mediation), or if the Mediator agreed upon is unable or unwilling to act, either party shall within ten (10) Working Days from the date of the proposal to appoint a Mediator or within ten (10) Working Days of notice to either party that he is unable or unwilling to act, apply to the Centre for Effective Dispute Resolution ('CEDR') to appoint a Mediator;
- 2.1.2 the CUSTOMER and the CONTRACTOR shall within ten (10) Working Days of the appointment of the Mediator meet with him in order to agree a programme for the exchange of all relevant information and the structure to be adopted for negotiations to be held. The parties may at any stage seek assistance from the CEDR to provide guidance on a suitable procedure.
- 2.2 Unless otherwise agreed by the CUSTOMER and the CONTRACTOR, all negotiations connected with the dispute and any settlement agreement relating to it shall be conducted in confidence and without prejudice to the rights of the parties in any future proceedings.
- 2.3 In the event that the CUSTOMER and the CONTRACTOR reach agreement on the resolution of the dispute, the agreement shall be reduced to writing and shall be binding on both parties once it is signed by the CUSTOMER's second point of contact Director of Service Delivery and the CONTRACTOR's second point of contact Service Delivery Manager.
- 2.4 Failing agreement, either the CUSTOMER or CONTRACTOR may invite the Mediator to provide a non-binding but informative opinion in writing. Such an opinion shall be provided on a without prejudice basis and shall not be used in evidence in any proceedings relating to this Contract without the prior written consent of both parties.

- 2.5 The CUSTOMER and the CONTRACTOR shall each bear their own costs in relation to any reference made to the Mediator and the fees and all other costs of the Mediator shall be borne jointly in equal proportions by both parties unless otherwise directed by the Mediator.
- 2.6 Work and activity to be carried out under this Contract shall not cease or be delayed during the mediation process.
- 2.7 In the event that the CUSTOMER and the CONTRACTOR fail to reach agreement in the structured negotiations within forty (40) Working Days of the Mediator being appointed, or such longer period as may be agreed, then any dispute or difference between them may, subject to the agreement of both parties, be referred to arbitration in accordance with the provisions of Clause 18.5.

### **3. ARBITRATION**

- 3.1 In the event that a dispute between the CUSTOMER and the CONTRACTOR, or a claim by one against the other, pursuant to the terms of this Contract is not resolved pursuant to paragraph 2 of this Schedule 2-9, the parties may, in accordance with the provisions of Clause 18.5, refer the matter to arbitration in accordance with this Schedule 2-9.
- 3.2 The party seeking to initiate the arbitration shall give a written Notice of Arbitration to the other party. The Notice of Arbitration shall specifically state:
- 3.2.1 that the dispute is referred to arbitration;
  - 3.2.2 the particulars of this Contract; and
  - 3.2.3 a brief summary of the subject of the dispute.
- 3.3 Unless otherwise agreed in writing by the CUSTOMER and the CONTRACTOR, the provisions of the Arbitration Act 1996 shall govern the arbitration commenced pursuant to this Schedule 2-9.
- 3.4 Any dispute arising out of or in connection with this Contract, including any question regarding its existence, validity or termination, if referred to arbitration in accordance with this Schedule 2-9 shall be resolved by arbitration under the procedural rules of the London Court of International Arbitration.
- 3.5 It is agreed between the CUSTOMER and the CONTRACTOR that for the purposes of the arbitration, the arbitrator shall have the power to make provisional awards as provided for in Section 39 of the Arbitration Act 1996.
- 3.6 For the avoidance of doubt it is agreed by the CUSTOMER and the CONTRACTOR that the arbitration process and anything said, done or produced in or in relation to the arbitration process (including any awards) shall be confidential between the parties, except as may be lawfully required in judicial proceedings relating to the arbitration or otherwise. No report relating to anything said, done or produced in or in relation to the arbitration process may be made to any body other than the tribunal, the CUSTOMER and the CONTRACTOR, their legal representatives and any person necessary to the conduct of the proceedings, without the agreement of all parties to the arbitration.
- 3.7 The arbitration proceedings shall take place in London and in the English language and the arbitration proceedings shall be governed by, and interpretations made in accordance with, English law.

- 3.8 The CUSTOMER and the CONTRACTOR shall each bear their own costs in relation to any reference made to the arbitrator and the fees and all other costs of the arbitrator shall be borne jointly in equal proportions by both parties unless otherwise directed by the arbitrator.
- 3.9 In the event that the CUSTOMER and the CONTRACTOR do not agree to refer the matter to arbitration, then any dispute or difference between them may be referred to the Courts in accordance with the provisions of Clause 33.

THIS PAGE IS INTENTIONALLY LEFT BLANK

---

**SCHEDULE 2-10**  
**STANDARDS AND REGULATIONS**

**1. INTRODUCTION**

- 1.1. This Schedule 2-10 sets out the Standards and Regulations with which the CONTRACTOR shall comply in its supply of the Ordered Goods and the provision of the Ordered Services.
- 1.2. References to the energy star criteria are set out in version 4 of the energy star program requirements for Computers. Please refer to [www.energystar.gov](http://www.energystar.gov)

**2. GENERAL STANDARDS**

- 2.1. The CONTRACTOR shall perform the Solution in accordance with the Specification Schedule 2.2
- 2.2. The CONTRACTOR shall meet or exceed the Service Level indicators in any given Service Period as defined in the Schedule 2-2 Service Levels.
- 2.3. The CONTRACTOR shall perform the Solution with reasonable care and diligence including but not limited to industry best practice (as defined by the OGC ([www.best-management-practice.com](http://www.best-management-practice.com))) and in accordance with its own established internal processes.
- 2.4. The CONTRACTOR warrants and represents that all staff assigned to the performance of the Solution shall possess and exercise the skill and experience, qualifications and expertise necessary for the proper performance of the Services.
- 2.5. In the event that the Service Definition does not specify particular Equipment or processes for use in the Solution the CONTRACTOR shall ensure that any equipment and processes are suitable for the performance of the Solution required and (unless the CUSTOMER'S Representative agrees otherwise) approved by the CUSTOMER.
- 2.6. The CONTRACTOR warrants and represents that it has full capacity and authority and all necessary consents (including, where relevant, the consent of its parent company) to enter into and perform this Contract and that this Contract has been executed by a duly authorised representative of the CONTRACTOR.
- 2.7. Quality Management System
  - 2.7.1. The CONTRACTOR shall undertake its obligations arising hereunder and in all Contracts in accordance with the BS EN ISO 9001 Quality Management System standard.
  - 2.7.2. The CONTRACTOR shall ensure that its Sub-Contractors undertake their obligations arising under Contracts in accordance with the BS EN ISO 9001 Quality Management System standard.

**3. TECHNICAL**

**3.1. eGovernment Interoperability Framework**

- 3.1.1. The CONTRACTOR shall comply with the appropriate sections of e-Government Interoperability Framework (e-GIF) and Government Metadata Standards (eGMS) for the delivery of the Ordered Goods and Ordered Services. Reference the latest version at:  
[www.govtalk.gov.uk/interoperability/egif.asp?order=title](http://www.govtalk.gov.uk/interoperability/egif.asp?order=title)

### 3.2. Technical Standards Catalogue

- 3.2.1. Data exported in the form of XML will comply with the W3C standards.
- 3.2.2. The CONTRACTOR shall use Open Systems Interconnection (OSI) or Internet Protocol Suite (IP) standards wherever possible.
- 3.2.3. Implementation of electronic mail systems shall be compatible with the GSI and/or xGSI standards as appropriate.
- 3.2.4. All equipment used to connect to the public telephone network shall have prior type approval by the British Approvals Board for Telecommunications (BABT) or an equivalent body within the European Union.
- 3.2.5. Where the CONTRACTOR is requested to carry out application development work the technical standards must be agreed with the CUSTOMER.

### 3.3. ITIL Guidelines

- 3.3.1. The CONTRACTOR shall follow the guidelines contained in the Office of Government Commerce's IT Infrastructure Library ("ITIL guidelines") for delivering the Ordered Services or may propose alternatives that are broadly functionally consistent with the ITIL3 or later guidelines.
- 3.3.2. The CONTRACTOR shall ensure that its service support processes include:
  - 3.3.2.1. Configuration Management
  - 3.3.2.2. Service Desk
  - 3.3.2.3. Incident Management
  - 3.3.2.4. Problem Management
  - 3.3.2.5. Change Management; and
  - 3.3.2.6. Release Management
- 3.3.3. The CONTRACTOR shall ensure that its service delivery processes include:
  - 3.3.3.1. Service Level Management;
  - 3.3.3.2. ICT Financial Management;
  - 3.3.3.3. Capacity Management;
  - 3.3.3.4. Availability Management;
  - 3.3.3.5. ICT Service Continuity Management; and
  - 3.3.3.6. Security Management.
- 3.3.4. The CONTRACTOR shall initiate a project within three months of the Effective Date with the aim of achieving ISO20000 (IT Service Management) certification within 18 months of the Effective Date. This certification is to apply to the service specified in the Agreement and not to the CONTRACTOR's organisation as a whole.
- 3.3.5. The CONTRACTOR shall on reasonable request allow the CUSTOMER to engage the services of a Registered Certification Body (RCB) to audit their compliance with the ISO20000 standard, provided that such audit shall be on reasonable notice to the CONTRACTOR, and shall not take place more frequently than once in any 12 month period and the cost of such audit is borne by the CUSTOMER.

3.3.6. The CONTRACTOR's ICT service management functions shall interface with the CUSTOMER in accordance with the CUSTOMER's ICT service management framework.

3.3.7. The CONTRACTOR shall on reasonable request provide the CUSTOMER with documents showing how ITIL guidelines have been followed in the provision of the Ordered Goods and Ordered Services.

3.3.8. The CONTRACTOR shall on request allow the CUSTOMER or its representatives to audit any or all of its ICT service management functions [to ensure that ITIL guidelines are being followed in the delivery of the Ordered Services.

#### 3.4.Environment

3.4.1. The CONTRACTOR undertakes to follow a sound environmental management policy so that its activities comply with all applicable environmental legislation and regulations and that its products or services are procured, produced, packaged, delivered and are capable of being used and ultimately disposed of, in ways that are appropriate from an environmental protection perspective.

3.4.2. The CONTRACTOR warrants that it has obtained ISO 14000/14001 certification for its environmental management and shall comply with and maintain such certification requirements.

3.4.3. The CONTRACTOR shall comply with relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2002/96/EC.

3.4.4. The CONTRACTOR shall ensure that all equipment procured to operate the managed service Solution meet the requirements of the Energy Star program and meet requirements for low energy consumption and reduce the amount of energy consumed through the life cycle, power management capability to be enabled on delivery and include sleep modes and off modes with capability of powering back up when required. References to the energy star criteria are set out in version 4 of the Energy Star program requirements. Please refer to [www.energystar.gov](http://www.energystar.gov)

#### 3.5.Project management

3.5.1. The CONTRACTOR shall generally make use of PRINCE2 methodology or similar, supplemented where appropriate by the tools and methods of the CONTRACTOR's own project management methodologies.

#### 3.6.Systems Development Environment

3.6.1. Any requirements analysis or requirements capture shall be based on Structured System Analysis and Design Methodology, (SSADM) or [Dynamic Systems Development Methodology (DSDM)] or equivalents (tailored where appropriate and necessary) as agreed with the CUSTOMER.

### 4. DATA STANDARDS

4.1.The CONTRACTOR shall develop, document, operate and maintain standards and procedures for ensuring the quality and integrity of all data. These standards and procedures must be agreed with the CUSTOMER.

4.2.The CONTRACTOR shall ensure that the authenticity of Records preserved over the long term (e.g. those for which the creating software has gone out of support) is sustained through their life cycle to support the presumption that the Records are what they purport to be and have not been modified or corrupted in essential respects. The Contractor shall ensure that Records will continue to possess the critical characteristics of authenticity, reliability, integrity and usability required by BS ISO 15489.

## 5. INFORMATION STANDARDS

5.1.The CONTRACTOR will have in place systems and procedures which will be subject to external audit for control over deliverable services or systems

5.2.Version control

5.2.1. The CONTRACTOR shall develop procedures which ensure that only the correct release or version of a Deliverable can be delivered to the CUSTOMER. The CONTRACTOR shall provide a copy of the draft procedures to the CUSTOMER for its approval. On receipt of such approval, the CONTRACTOR shall then operate those procedures.

## 6. HEALTH AND SAFETY STANDARDS

6.1.The CONTRACTOR shall ensure that all IT equipment provided complies with the Electromagnetic Compatibility Regulations 1992, No. 2372.

6.2.The CONTRACTOR shall ensure that they meet the following standards and regulations, and adhere to the following measurement techniques, or their replacements in the event of their being superseded, for the term of this Agreement:

**Table 5**

<b>Description</b>	<b>Standard</b>
Ergonomic requirements for office work with visual display terminals (VDTs)	BS EN ISO 9241 (All parts including BS EN 29241-2 and BS EN 29241-3)
Noise emitted by computer and business equipment	BS 7135-2:1989, BS 7135-3:1989,
Acoustics - Measurement of airborne noise emitted by information technology and telecommunications equipment	BS EN ISO 7779:2001
Particular safety requirements for equipment to be connected to telecommunication networks	BS EN 41003:1999
Electromagnetic Compatibility. Generic immunity standard. Part 1. Residential, commercial and light industry	BS EN 50082-1:1998
Specification for Uninterruptible power systems (UPS). Part 2. EMC requirements	BS EN 50091-2:1996
Electromagnetic Compatibility - Requirements for household appliances, electric tools and similar apparatus. Part 1: Emissions	BS EN 55014-1:2001
Information technology equipment - Radio disturbance characteristics – Limits and methods of measurement	BS EN 55022:1998
Audio, video and similar electronic apparatus – Safety requirements	BS EN 60065:2002
Electromagnetic Compatibility for industrial-process measurement and control equipment. Part 2: Electrostatic	BS EN 60801-2:1993

## ICT GOODS AND ASSOCIATED SERVICES

Description	Standard
discharge requirements	
Safety of Laser Products Part 1: Equipment classification, requirements and user's guides. Part 2: Safety of optical fibre communication systems	BS EN 60825-1:1994 BS EN 60825-2:2000
Information technology equipment – Safety – Part 1: General requirements	BS EN 60950-1:2002
Electromagnetic compatibility (EMC). Part 6-1: Generic standards. Immunity for residential, commercial and light industrial environments. Part 6-2: Generic standards. Immunity standard for Industrial environments. Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments.	BS EN 61000-6-1:2001 BS EN 61000-6-2:2001 BS EN 61000-6-3:2001
Uninterruptible power systems (UPS) – Part 1-1: General and safety requirements for UPS used in operator access areas	BS EN 62040-1-1:2003

7. In the event of a standard being modified or superseded during the duration of the agreement, the CONTRACTOR shall inform the CUSTOMER within twenty (20) working days of any impact of the change on the delivery of services.

7.1. The Tendered Contract will be established on the terms and conditions of the Model Contract for ICT Goods and Services Model Agreement v6.0 and will incorporate the following statutory obligations (or their European equivalent).

7.1.1. Income and Corporation Taxes Act 1988

7.1.2. Section 12 of the Sale of Goods Act 1979 or Section 2 of the Supply of Goods and Services Act 1982

7.1.3. Schedule 1 of the Data Protection Act 1998

7.1.4. The OHSAS 18001 Occupational Health and Safety Management System

7.1.5. The Sex Discrimination Act 1975,

7.1.6. The Race Relations Act 1976, the Disability Discrimination Act 1995,

7.1.7. The Employment Equality (Religion or Belief) Regulations 2003

7.1.8. The Employment Equality (Sexual Orientation) Regulations 2003

7.1.9. Data protection requirements: Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003

7.1.10. BS EN ISO 9001 Quality Management System standard.

7.1.11. COSHH regulations or the Montreal Protocol

7.1.12. The Private Security Industry Act 2001

7.1.13. Directive 2002/96/EC on Waste Electrical and Electronic Equipment and Directive 2002/95/EC on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment

7.1.14. National Audit Act 1983 or otherwise.

THIS PAGE IS INTENTIONALLY LEFT BLANK

---

**SCHEDULE 2-11**

**LIQUIDATED DAMAGES**

**NOT USED**

**SCHEDULE 2-12**

**MODEL CONFIDENTIALITY AGREEMENT**

**1. INTRODUCTION**

- 1.1. This Schedule 2-12 contains Model Confidentiality Agreements.
- 1.2. Model Confidentiality Agreement (1) is appropriate for the provisions of Clause 16.4.1; and
- 1.3. Model Confidentiality Agreement (2) is appropriate for the provisions of Clause 16.4.2.

MODEL CONFIDENTIALITY AGREEMENT (1)

This Confidentiality Agreement is made on the [ ] day of [ ] 200[ ] between:

- A) [ ] (“the CUSTOMER”); and  
B) [ ] (“the RECIPIENT”)

**WHEREAS:**

- 1) The CUSTOMER has entered into a Contract with [name] (“the CONTRACTOR”);
- 2) This Confidentiality Agreement is pursuant to the provisions of Clause 16.4.1 of the Contract;
- 3) the RECIPIENT is a Crown Body; and
- 4) the CUSTOMER may have made available and may wish to make available to the RECIPIENT certain Confidential Information (as defined below). The CUSTOMER wishes to protect such information in the manner set out in this Confidentiality Agreement.

In consideration of the mutual promises contained herein, **IT IS HEREBY AGREED AS FOLLOWS:-**

**1. DEFINITIONS**

- 1.1. “Confidential Information” means any information, however it is conveyed, received by the RECIPIENT from the CUSTOMER that relates to the business, affairs, developments, trade secrets, know-how, personnel and suppliers of either party, including Intellectual Property Rights, of the CONTRACTOR together with all information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as “confidential”) or which ought reasonably to be considered to be confidential.
- 1.2. “Party” means either party to this Confidentiality Agreement as specified in A), and B) above.

**2. HANDLING OF CONFIDENTIAL INFORMATION**

- 2.1. The RECIPIENT shall, and shall ensure and procure that its servants shall, maintain the Confidential Information in strict confidence, including requiring its servants to enter into a confidentiality agreement on substantially the same terms as this Confidentiality Agreement, and shall, without limitation to the generality of this obligation, exercise in relation thereto no less security measures and degree of care than those which it applies to its own confidential information which it warrants as providing adequate protection against unauthorised disclosure, copying or use.
  - 2.2. Upon termination of this Confidentiality Agreement, all Confidential Information received by the RECIPIENT and copies thereof shall be destroyed by him.
-

**3. THE RECIPIENT OBLIGATIONS**

- 3.1. The RECIPIENT shall:-
  - 3.1.1. not divulge the Confidential Information to any third Party other than as provided for in this Confidentiality Agreement; and
  - 3.1.2. make no commercial use of the Confidential Information or any part thereof.
- 3.2. Notwithstanding the foregoing, the RECIPIENT shall be entitled to make any disclosure required by law of the Confidential Information and shall notify the CUSTOMER of so doing in accordance with the provisions of paragraph 6.

**4. EXCLUSIONS**

- 4.1. This Confidentiality Agreement shall not apply to information which:
  - 4.1.1. is or becomes public knowledge without breach of this Confidentiality Agreement; or
  - 4.1.2. is already in the possession of the RECIPIENT without restriction in relation to disclosure before the date of its receipt with restriction from the CUSTOMER; or
  - 4.1.3. is received by the RECIPIENT from a third party who lawfully acquired it and who is under no obligation restricting its disclosure.
  - 4.1.4. must be disclosed pursuant to a statutory, legal or parliamentary obligation placed upon the party making the disclosure, including any requirements for disclosure under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004.
- 4.2. Notwithstanding the provisions of paragraph 4.1.2, where information disclosed to the RECIPIENT by the CUSTOMER without restriction is subsequently disclosed by the CUSTOMER with restriction, the RECIPIENT shall treat such information in accordance with the provisions of this Confidentiality Agreement with effect from the date of its disclosure with restriction. In all such cases, the parties shall use all reasonable endeavours to restore and maintain the confidentiality of that information.

**5. DISCLAIMER**

- 5.1. All rights in Confidential Information are reserved and no rights or obligations other than those expressly recited herein are granted or to be implied from this Confidentiality Agreement.
- 5.2. In particular, no licence or other interest is hereby granted directly or indirectly under any invention, discovery, patent, design right, copyright or other industrial property right now or in the future held, made, obtained or licensable by the CUSTOMER or the CONTRACTOR.

**6. NOTICES**

---

- 6.1. Except as otherwise expressly provided, no communication from one Party to the other shall have any validity under this Confidentiality Agreement unless made in writing by or on behalf of the relevant Party.

**7. TERMINATION**

- 7.1. This Confidentiality Agreement shall continue in force until terminated by consent of the parties. The provisions of paragraphs 1, 2, 3 and 4 shall survive any such termination.

**8. NON-ASSIGNMENT**

- 8.1. This Confidentiality Agreement is personal to the RECIPIENT and shall not be assigned or otherwise transferred in whole or in part by the RECIPIENT.

**9. ENTIRE AGREEMENT**

- 9.1. This Confidentiality Agreement constitutes the entire agreement and understanding between the parties in respect of Confidential Information and supersedes all previous agreements, understandings and undertakings in such respect.
- 9.2. As witness this Confidentiality Agreement has been executed on behalf of each Party by its duly authorised representative on the date first above written.

**10. THIRD PARTY RIGHTS**

- 10.1. Except where expressly provided to the contrary, this Confidentiality Agreement is not intended to be for the benefit of, and shall not be enforceable by, any person who is not named at the date of this Confidentiality Agreement as a party to it, or any person who claims rights under the Contracts (Rights of Third Parties) Act 1999 or otherwise and neither party can declare itself a trustee of the rights under it for the benefit of any third party. The parties to this Confidentiality Agreement reserve the right to rescind or vary this Confidentiality Agreement without the consent of any third party who is expressly entitled to enforce this Confidentiality Agreement.
- 10.2. The Parties acknowledge that the rights set out in this Confidentiality Agreement may be enforced by the CONTRACTOR.

For the RECIPIENT:

Signed by: \_\_\_\_\_

Date: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

---

## ICT GOODS AND ASSOCIATED SERVICES

---

For the CUSTOMER:

Signed by: \_\_\_\_\_

Date: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

---

MODEL CONFIDENTIALITY AGREEMENT (2)

This Confidentiality Agreement is made on the [ ] day of [ ] 200[ ] between:

- A) [ ] (“the CUSTOMER”); and  
B) [ ] (“the THIRD PARTY”)

WHEREAS:

- 1) The CUSTOMER has entered into a Contract with [name] (“the CONTRACTOR”);
- 2) This Confidentiality Agreement is pursuant to the provisions of Clause 16.4.2 of the Contract;
- 3) the CUSTOMER has engaged the THIRD PARTY to provide services related to that Contract;
- 4) the CUSTOMER may have made available and may wish to make available to the THIRD PARTY certain Confidential Information (as defined below). The CUSTOMER wishes to protect such information in the manner set out in this Confidentiality Agreement.

In consideration of the mutual promises contained herein, **IT IS HEREBY AGREED AS FOLLOWS:-**

**1. DEFINITIONS**

- 1.1. “Confidential Information” means any information, however it is conveyed, received by the THIRD PARTY from the CUSTOMER that relates to the business, affairs, developments, trade secrets, know-how, personnel and suppliers of either party, including Intellectual Property Rights, of the CONTRACTOR together with all information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as “confidential”) or which ought reasonably to be considered to be confidential.
- 1.2. “Party” means either party to this Confidentiality Agreement as specified in A), and B) above.

**2. HANDLING OF CONFIDENTIAL INFORMATION**

- 2.1. The THIRD PARTY shall, and shall ensure and procure that its servants shall, maintain the Confidential Information in strict confidence, including requiring its servants to enter into a confidentiality agreement on substantially the same terms as this Confidentiality Agreement, and shall, without limitation to the generality of this obligation, exercise in relation thereto no less security measures and degree of care than those which it applies to its own confidential information which it warrants as providing adequate protection against unauthorised disclosure, copying or use.
  - 2.2. Upon termination of this Confidentiality Agreement, all Confidential Information received by the THIRD PARTY and copies thereof shall be destroyed by him.
-

**3. THIRD PARTY OBLIGATIONS**

- 3.1. The THIRD PARTY shall:-
  - 3.1.1. not divulge the Confidential Information to any party other than as provided for in this Confidentiality Agreement;
  - 3.1.2. use the Confidential Information only for the purposes necessary in providing the services for which he is engaged by the CUSTOMER; and
  - 3.1.3. make no commercial use of the Confidential Information or any part thereof.
- 3.2. Notwithstanding the foregoing, the THIRD PARTY shall be entitled to make any disclosure required by law of the Confidential Information and shall notify the CUSTOMER of so doing in accordance with the provisions of paragraph 6.

**4. EXCLUSIONS**

- 4.1. This Confidentiality Agreement shall not apply to information which:
  - 4.1.1. is or becomes public knowledge without breach of this Confidentiality Agreement; or
  - 4.1.2. is already in the possession of the THIRD PARTY without restriction in relation to disclosure before the date of its receipt with restriction from the CUSTOMER; or
  - 4.1.3. is received by the THIRD PARTY from a third party who lawfully acquired it and who is under no obligation restricting its disclosure.
- 4.2. Notwithstanding the provisions of paragraph 4.1.2, where information disclosed to the THIRD PARTY by the CUSTOMER without restriction is subsequently disclosed by the CUSTOMER with restriction, the THIRD PARTY shall treat such information in accordance with the provisions of this Confidentiality Agreement with effect from the date of its disclosure with restriction. In all such cases, the Parties shall use all reasonable endeavours to restore and maintain the confidentiality of that information.

**5. DISCLAIMER**

- 5.1. All rights in Confidential Information are reserved and no rights or obligations other than those expressly recited herein are granted or to be implied from this Confidentiality Agreement.
- 5.2. In particular, no licence or other interest is hereby granted directly or indirectly under any invention, discovery, patent, design right, copyright or other industrial property right now or in the future held, made, obtained or licensable by the CUSTOMER or the CONTRACTOR.

**6. NOTICES**

---

- 6.1. Except as otherwise expressly provided, no communication from one Party to the other shall have any validity under this Confidentiality Agreement unless made in writing by or on behalf of the relevant Party.

**7. TERMINATION**

- 7.1. This Confidentiality Agreement shall continue in force until terminated by consent of the Parties. The provisions of paragraphs 1, 2, 3 and 4 shall survive any such termination.

**8. NON-ASSIGNMENT**

- 8.1. This Confidentiality Agreement is personal to the THIRD PARTY and shall not be assigned or otherwise transferred in whole or in part by the THIRD PARTY.

**9. ENTIRE AGREEMENT**

- 9.1. This Confidentiality Agreement constitutes the entire agreement and understanding between the Parties in respect of Confidential Information and supersedes all previous agreements, understandings and undertakings in such respect.
- 9.2. As witness this Confidentiality Agreement has been executed on behalf of each Party by its duly authorised representative on the date first above written.

**10. THIRD PARTY RIGHTS**

- 10.1. Except where expressly provided to the contrary, this Confidentiality Agreement is not intended to be for the benefit of, and shall not be enforceable by, any person who is not named at the date of this Confidentiality Agreement as a party to it, or any person who claims rights under the Contracts (Rights of Third Parties) Act 1999 or otherwise and neither party can declare itself a trustee of the rights under it for the benefit of any third party. The parties to this Confidentiality Agreement reserve the right to rescind or vary this Confidentiality Agreement without the consent of any third party who is expressly entitled to enforce this Confidentiality Agreement.
- 10.2. The Parties acknowledge that the rights set out in this Confidentiality Agreement may be enforced by the CONTRACTOR.

For the THIRD PARTY:

Signed by: \_\_\_\_\_

Date: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

---

## ICT GOODS AND ASSOCIATED SERVICES

---

For the CUSTOMER:

Signed by: \_\_\_\_\_

Date: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

---

**SCHEDULE 2-13**  
**SECURITY REQUIREMENTS AND PLAN**

**1. INTRODUCTION**

1.1. This schedule covers:

- 1.1.1. principles of security for the CONTRACTOR Solution, derived from the Security Policy, including without limitation principles of physical and information security;
- 1.1.2. wider aspects of security relating to the Ordered Goods and Ordered Services;
- 1.1.3. the creation of the Security Plan;
- 1.1.4. audit and testing of the Security Plan;
- 1.1.5. conformance to ISO/IEC:27002 (Information Security Code of Practice) and ISO/IEC 27001 (Information Security Requirements Specification) (Standard Specification);
- 1.1.6. management of Security Incidents;
- 1.1.7. managing information assurance;
- 1.1.8. governance of the Security Policy;
- 1.1.9. protective markings and asset control;
- 1.1.10. personnel security;
- 1.1.11. information security;
- 1.1.12. physical security; and
- 1.1.13. other security measures.

**2. PRINCIPLES OF SECURITY**

- 2.1. The CONTRACTOR acknowledges that the CUSTOMER places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the sites and the security for the CONTRACTOR Solution. The CONTRACTOR also acknowledges the confidentiality of the CUSTOMER's Data
- 2.2. 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 produced by the CONTRACTOR fully complies with the Security Policy.
- 2.3. The CUSTOMER shall notify the CONTRACTOR of any changes or proposed changes to the Security Policy.

- 2.4. If the CONTRACTOR believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the Ordered Goods and Ordered Services, it may submit a request in accordance with the Contract Change Procedure detailed at Schedule 2-7. 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 to mitigate those costs. Any change to the Charges shall then be agreed in accordance with the Contract Change Procedure.
- 2.5. Until and/or unless a change to the Charges is agreed by the CUSTOMER, pursuant to clause 8.1 of this Contract, the CONTRACTOR shall continue to provide the Ordered Goods and Ordered Services in accordance with its existing obligations.
- 2.6. The CONTRACTOR shall be responsible for the security of the CONTRACTOR's Solution and shall at all times provide a level of security which:
- 2.6.1. is in accordance with Good Industry Practice, HMG Practice and the Law;
  - 2.6.2. complies with the Security Policy as outlined in Appendix 2;
  - 2.6.3. complies with the HMG Security Policy Framework and any subsequent revisions or replacements of that framework to the extent agreed between the parties during the Term, with any significant requirements (not included in the Security Plan to be agreed prior to Service Commencement Date) to be undertaken in accordance with the Contract Change Procedures. Any request for compliance that goes beyond those reasonably required for the purposes of the Solution will be undertaken in accordance with the Contract Change Procedure;
  - 2.6.4. complies with all HMG Information Security Standards and any subsequent revisions, replacements or new inclusions of those standards to the extent agreed between the parties during the Term, with any significant requirements (not included in the Security Plan to be agreed prior to Service Commencement Date) to be undertaken in accordance with the Contract Change Procedures. Any request for compliance that goes beyond those reasonably required for the purposes of the Solution will be undertaken in accordance with the Contract Change Procedure;
  - 2.6.5. meets any specific security threats to the CONTRACTOR's Solution; and
  - 2.6.6. complies with ISO/IEC27002 and ISO/IEC27001 in accordance with paragraph 6 of this schedule.
- 2.7. Without limiting paragraph 2.6, the CONTRACTOR shall at all times ensure that the level of security employed in the provision of the Ordered Goods and Ordered Services is appropriate to maintain the following at acceptable risk levels (to be defined by the CUSTOMER in the Security Plan):
- 2.7.1. loss of integrity of CUSTOMER Data;
  - 2.7.2. loss of confidentiality of CUSTOMER Data;

- 2.7.3. unauthorised access to, use of, or interference with CUSTOMER Data by any person or organisation;
- 2.7.4. unauthorised access to network elements, buildings, the CUSTOMER premises, and tools used by the CONTRACTOR in the provision of the Ordered Services;
- 2.7.5. use of the CONTRACTOR Solution or Order Goods and Ordered Services by any third party in order to gain unauthorised access to any computer resource or CUSTOMER Data; and
- 2.7.6. loss of availability of CUSTOMER Data due to any failure or compromise of the Ordered Goods and Ordered Services.

### **3. SECURITY PLAN**

#### **3.1. Introduction**

- 3.1.1. The CONTRACTOR shall develop, implement and maintain a Security Plan to apply during the Term (and after the end of the Term (as applicable) in accordance with Schedule 2-14 (Exit and Service Transfer) and the Service Transfer Plan which will be approved by the CUSTOMER, tested, periodically updated and audited in accordance with this schedule.
- 3.1.2. When developing the Security Plan, the CONTRACTOR must consult with the CUSTOMER's Security Officer or their representative.
- 3.1.3. An example Security Plan has been included in Appendix 1. The CONTRACTOR may set out their Security Plan in accordance with that Appendix or in some other form, as agreed with the CUSTOMER.

#### **3.2. Development**

- 3.2.1. Within 90 Days after the Effective Date and in accordance with paragraph 3.4 (Amendment and Revision), the CONTRACTOR will prepare and deliver to the CUSTOMER for approval the full and final Security Plan.
- 3.2.2. If the Security Plan is approved by the CUSTOMER it will be adopted immediately. If the Security Plan is not approved by the CUSTOMER the CONTRACTOR shall amend it within 10 Working Days of a notice of non-approval from the CUSTOMER and re-submit to the CUSTOMER for approval. The parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the CUSTOMER. If the CUSTOMER does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the CUSTOMER pursuant to this paragraph 3.2.2 of this schedule 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 set out in paragraphs 3.1.1 to 3.3.4 shall be deemed to be reasonable.

**3.3. Content**

- 3.3.1. The Security Plan will set out the security measures to be implemented and maintained by the CONTRACTOR in relation to all aspects of the Ordered Goods and Ordered Services and all processes associated with the delivery of the Ordered Goods and Ordered Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Ordered Goods and Ordered Services comply with:
- 3.3.1.1. the provisions of this schedule;
  - 3.3.1.2. the provisions of schedule 2.2 (The Ordered Goods, Ordered Services, Service Levels and Service Credits) relating to security;
  - 3.3.1.3. The HMG Security Policy Framework and any subsequent revisions or replacements.
  - 3.3.1.4. ISO/IEC27002 and ISO/IEC27001;
  - 3.3.1.5. the data protection compliance guidance produced by the CUSTOMER;
  - 3.3.1.6. appropriate ICT standards for technical countermeasures which are included in the CONTRACTOR System;
  - 3.3.1.7. encryption standards in accordance with the current standards and guidance issued by CESG;
  - 3.3.1.8. the Risk Management Accreditation Document Set (RMADS);
  - 3.3.1.9. the Information Assurance Maturity Model (IAMM);
  - 3.3.1.10. the Government Protective Marking Scheme (GPMS);
  - 3.3.1.11. all HMG Information Security Standards (IS) and any new inclusions of those standards; and
  - 3.3.1.12. PCI Data Security Standards (PCI DSS) as required as a processor of credit transactions.
- 3.3.2. The references to standards, guidance and policies set out in paragraph 3.3.1 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.
- 3.3.3. In the event of any inconsistency in the provisions of the above standards, guidance and policies, the CONTRACTOR should notify the CUSTOMER's Representative of such inconsistency immediately upon becoming aware of the same, and the CUSTOMER's Representative shall, as soon as practicable, advise the CONTRACTOR which provision the CONTRACTOR shall be required to comply with.
- 3.3.4. The Security Plan shall be written in plain English in language which is readily comprehensible to the staff of the CONTRACTOR and the CUSTOMER engaged in the Ordered Goods and Ordered Services and shall not reference any other documents which are not either in the possession of the CUSTOMER or otherwise specified in this schedule.

3.4. Amendment and Revision

3.4.1. The Security Plan will be fully reviewed and updated by the CONTRACTOR annually, or from time to time to reflect:

3.4.1.1. emerging changes good industry practice, HMG Practice and the Law;

3.4.1.2. any change or proposed change to the CONTRACTOR System, the Ordered Services and/or associated processes;

3.4.1.3. any new perceived or changed threats to the CONTRACTOR's System as identified by either the CONTRACTOR or the CUSTOMER; and

3.4.1.4. a reasonable request by the CUSTOMER.

3.4.2. The CONTRACTOR will provide the CUSTOMER 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 CUSTOMER.

3.4.3. Any change or amendment which the CONTRACTOR proposes to make to the Security Plan (as a result of a CUSTOMER request or change to the Schedule 2.2 (The Ordered Services) or otherwise shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the CUSTOMER.

**4. AUDIT AND TESTING**

4.1. 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 CUSTOMER.

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

4.3. Without prejudice to any other right of audit or access granted to the CUSTOMER pursuant to this Contract, the CUSTOMER shall be entitled at any time and with the consent of the CONTRACTOR not to be unreasonably withheld to carry out such tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the CONTRACTOR's compliance with and implementation of the Security Plan. Such tests will be conducted using appropriately qualified testers at the cost of the CUSTOMER. The CUSTOMER 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 delivery of the Ordered Goods and Ordered Services. If such tests impact adversely on its ability to deliver the Ordered Goods and Ordered Services to the agreed Service Levels, the CONTRACTOR shall be granted relief against any resultant under-performance for the period of the tests. The CONTRACTOR accepts no responsibility for the CUSTOMER's testers that gain access to protectively marked material beyond their personal level of clearance or their need to know in conducting such tests.

4.4. Where any Security Test carried out pursuant to paragraphs 4.2 or 4.3 above reveals any actual or potential security failure or weaknesses, the CONTRACTOR on notification of such a failure or weakness shall promptly notify the CUSTOMER of any changes to the Security Plan (and the implementation thereof) which the CONTRACTOR proposes to make in order to correct such failure or weakness. Subject to the CUSTOMER's approval in accordance with paragraph 3.4.3, the CONTRACTOR shall implement such changes to the Security Plan in accordance with the timetable agreed with the CUSTOMER or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan to address a non-compliance with the Security Policy or security requirements, the change to the Security Plan shall be at no additional cost to the CUSTOMER. For the purposes of this paragraph 4, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements

## **5. REPORTING**

5.1. The CONTRACTOR must provide reports as requested by the CUSTOMER in relation to any information that is mentioned in this schedule.

5.2. The CONTRACTOR must provide such reports in a timely manner and in a format that will be notified to the CONTRACTOR by the CUSTOMER, but not in a way that interferes with the operation of the Ordered Service. The CUSTOMER may not make any requests under paragraph 5.1 that are unreasonable.

## **6. COMPLIANCE WITH ISO/IEC 27001**

6.1. The CONTRACTOR shall ensure that the security of the Solution conforms to ISO 27001 as soon as reasonably practicable and will maintain such conformity for the duration of the Agreement.

- 6.2. The CONTRACTOR shall maintain the security of the Solution to a standard which it reasonably believes that if independently tested, would meet the requirements for ISO 27001 certification.
- 6.3. For the avoidance of any doubt, the CONTRACTOR is not required to obtain independent certification of the security of the Solution to ISO 27001. Should the requirement of certification under ISO 27001 become mandatory, this sub-paragraph becomes void.
- 6.4. If certain parts of the security of the Solution do not conform to good industry practice as described in ISO 27002 and, as a result, the CONTRACTOR reasonably believes that if independently tested, the certification to ISO 27001 would fail in regard to these parts, the CONTRACTOR shall promptly notify the CUSTOMER of this and the CUSTOMER in its absolute discretion may waive the requirement for certification in respect of the relevant parts.
- 6.5. 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 Ordered Services in compliance with security aspects of ISO 27001 and shall promptly provide to the CUSTOMER any associated security audit reports and shall otherwise notify the CUSTOMER of the results of such security audits.
- 6.6. If it is the CUSTOMER's reasonable opinion that compliance with the principles and practices of ISO 27001 is not being achieved by the CONTRACTOR, then the CUSTOMER 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. If the CONTRACTOR does not become compliant within the required time then the CUSTOMER has the right to obtain an independent audit against these standards in whole or in part.
- 6.7. If, as a result of any such independent audit as described in paragraph 6.6 the CONTRACTOR is found to be non-compliant with the principles and practices of ISO 27001 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 CUSTOMER in obtaining such audit.

## **7. MANAGEMENT OF SECURITY INCIDENTS**

- 7.1. Either party shall notify the other immediately upon becoming aware of any Security Incidents including, but not limited to an actual, potential or attempted breach, or threat to, the Solution and/or the Security Plan.
- 7.2. Upon becoming aware of any of the circumstances referred to in paragraph 7.1, the CONTRACTOR shall:
  - 7.2.1. immediately take all reasonable steps necessary to:
    - 7.2.1.1. remedy such breach or protect the CONTRACTOR System against any such potential or attempted breach or threat; and
    - 7.2.1.2. prevent an equivalent breach in the future.

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

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

## **8. MANAGE INFORMATION ASSURANCE**

8.1. There is a requirement to provide a Solution to support the CUSTOMER's information assurance, encompassing risk management, accreditation and compliance with the HMG Security Policy Framework and associated standards.

## **9. GOVERNANCE OF SECURITY POLICY IN ACCORDANCE WITH THIS SCHEDULE.**

9.1. The CONTRACTOR shall demonstrate how the Ordered Services and Solution complies with the Cross Government: Mandatory Minimum Measures as set out in the Security Policy Framework

9.2. The CONTRACTOR shall maintain compliance with the Cross Government: Mandatory Minimum Measures as set in the Security Policy Framework as they are revised or replaced during the term of the Contract.

9.3. The CONTRACTOR shall maintain compliance with HMG IA Standards as the standards are revised during the term of the Contract

9.4. The CONTRACTOR shall, implement and act in accordance with the security policies, as defined in the HMG Security Policy Framework.

9.5. The CONTRACTOR shall ensure that all staff are aware of their responsibilities in relation to information security.

9.6. The CONTRACTOR shall provide initial and ongoing security awareness training to all of its employees and Sub-contractors..

9.7. The CONTRACTOR shall provide clear guidance to its employees on the disciplinary process for deliberately breaching information security management processes and systems.

9.8. The CONTRACTOR shall designate a representative to effectively manage and monitor the adherence to security measures and policies as required by the CUSTOMER.

9.9. The CONTRACTOR shall ensure that all new systems are accredited for security and information assurance and comply with the latest HMG Information Security Standards in place at the time of accreditation.

- 9.10. The CONTRACTOR shall allow the Accreditor or designated representative from the CUSTOMER to investigate, audit and report on the level of compliance by the CONTRACTOR to HMG Information Security standards.
- 9.11. The CONTRACTOR shall ensure that all Security Incidents are reported to the CUSTOMER as reasonably practical in the circumstances in line with the agreed timescales depending on criticality as set out in the Security Plan.
- 9.12. The CONTRACTOR shall ensure that the managed service Solution is capable of producing records of user activity to support monitoring, Incident response and investigations.
- 9.13. The CONTRACTOR shall develop and implement a Solution to monitor use of systems and services by users to support Incident response and investigations.
- 9.14. The CONTRACTOR shall ensure that a Disaster Recovery test of the IT systems is made annually and that the CUSTOMER is provided with a report following such tests.
- 9.15. The CONTRACTOR shall allow the CUSTOMER or those instructed by the CUSTOMER to complete a security audit to ensure compliance with HMG Information Security standards and the HMG Security Policy Framework.
- 9.16. The CONTRACTOR shall ensure that any sub-contractor engaged on the CUSTOMER's contract fully complies with HMG Information Security standards.
- 9.17. The CONTRACTOR shall hold interim meetings at agreed intervals to discuss information security risk, accreditation and compliance to HMG Information Security standards with the CUSTOMER's Security Officer and other relevant Stakeholders.

## **10. PROTECTIVE MARKING AND ASSET CONTROL**

- 10.1. The CONTRACTOR shall develop and maintain a Risk Management and Accreditation Document Set (RMADS) for the Ordered Service and Solution as defined in HMG IA Standard No 2.
- 10.2. The CONTRACTOR shall engage with risk management and accreditation activities throughout the lifetime of the contract with the CUSTOMER. The engagement will include but is not limited to:
- 10.2.1. During development, testing and release of each component of the Ordered Service & Solution.
- 10.2.2. At post implementation review and benefits realisation review.
- 10.2.3. On de-commissioning and handover at end of contract (as part of the Service Transfer Plan).
- 10.3. The CONTRACTOR shall develop and implement procedures for handling, processing, storing communicating and destroying information to provide protection appropriate to its level of sensitivity or protective marking.

- 10.4. The CONTRACTOR shall ensure physical media in transit is protected in a manner appropriate to its level of sensitivity or protective marking.
- 10.5. The CONTRACTOR shall ensure that its employees label and handle information according to its level of sensitivity and protective marking.
- 10.6. The CONTRACTOR shall provide an audit logging Solution that protects logs according to their levels of sensitivity or protective marking.
- 10.7. The CONTRACTOR shall mark all CUSTOMER owned hardware components with an SIA Asset Tag.

## **11. PERSONNEL SECURITY**

- 11.1. The CONTRACTOR shall ensure that all requirements of the Security Aspects Letter are complied with.
- 11.2. The CONTRACTOR shall ensure that all staff deployed on the CUSTOMER's activity sign a confidentiality agreement, and are security cleared to the appropriate level.
- 11.3. The CONTRACTOR shall ensure that equipment maintenance personnel have achieved the appropriate level of security clearance required for their role.
- 11.4. The CONTRACTOR shall ensure they withdraw all access rights and permissions from any system user on termination of their employment.

## **12. INFORMATION SECURITY**

- 12.1. The CONTRACTOR shall ensure that where Software is used in mobile, remote or home working situations by CONTRACTOR staff, that effective and appropriate security controls are employed.
- 12.2. The CONTRACTOR shall ensure the security of networks and network services deployed in the Ordered Service Solution.
- 12.3. The CONTRACTOR shall ensure the secure disposal of information to reduce the risk of information leakage of sensitive information.
- 12.4. The CONTRACTOR shall ensure that information contained in any electronic messaging system is protected according to its sensitivity or protective marking.
- 12.5. The CONTRACTOR shall ensure that effective security measures are implemented to control and monitor customer access to and use of the CUSTOMER's systems.
- 12.6. The CONTRACTOR shall provide users with access to only those IT and network resources required for their role.
- 12.7. The CONTRACTOR shall provide a formal registration procedure to grant and revoke users access to systems, services and information.
- 12.8. The CONTRACTOR shall review user privileges and access rights on at least an annual basis and on each change of user role. Revoking access when no longer required.

- 12.9. The CONTRACTOR shall provide an appropriate level of protection for remote access to systems and services.
- 12.10. The CONTRACTOR shall limit user access to information and applications according to their business requirement.
- 12.11. The CONTRACTOR shall limit the services available to users on shared or connected systems to those required to meet the business requirement.
- 12.12. The CONTRACTOR shall ensure there is separation between development, test, training and live systems to prevent accidental or deliberate compromise of operational information and systems.
- 12.13. The CONTRACTOR shall ensure there are effective controls in place to protect against malicious code.
- 12.14. The CONTRACTOR shall provide secure log-on procedures for access to systems and services.
- 12.15. The CONTRACTOR shall ensure that there are effective controls in place to manage the risks associated with interconnecting information systems and to limit those information exchanges to those required to meet the business requirement.
- 12.16. The CONTRACTOR shall ensure there are technical controls to protect against accidental or deliberate leakage of information from the Ordered Service Solution.
- 12.17. The CONTRACTOR shall protect physical records in accordance with all applicable legislation and as required by the CUSTOMER.
- 12.18. The CONTRACTOR shall protect all personal information and data in accordance with all applicable legislation, regulation and contracts.
- 12.19. The CONTRACTOR shall ensure that all technical connections with interfacing Stakeholders are accredited by the CUSTOMER's Security Officer or their representative.
- 12.20. The CONTRACTOR shall ensure that all interfacing codes of connection are formally agreed with interfacing Stakeholders.
- 12.21. The CONTRACTOR shall ensure that formal CHECK approved vulnerability analysis and penetration testing is undertaken as part of the initial risk management and accreditation process and at least annually during the term of the contract.
- 12.22. The CONTRACTOR shall agree the scope and requirements for penetration testing with the CUSTOMER and provide a copy of test report findings and actions required.
- 12.23. The CONTRACTOR shall provide access and assistance to the CUSTOMER's staff (or their representatives) to complete independent penetration testing of the Ordered Service Solution at times to be notified by the CUSTOMER.

### **13. PHYSICAL SECURITY**

- 13.1. The CONTRACTOR shall ensure that physical security controls are implemented and enforced for all operating sites, within buildings and specifically in rooms where sensitive information is processed or where equipment is located.
- 13.2. The CONTRACTOR shall ensure that equipment and supporting utilities and cabling are protected against any environmental risks or risks posed by external action.
- 13.3. The CONTRACTOR shall ensure there are physical and procedural controls in place to prevent the unauthorised removal of systems, equipment, storage devices, electronic media and other information assets from CONTRACTOR sites engaged in the CUSTOMER's business.
- 13.4. The CONTRACTOR shall ensure there are procedures in place to screen all mail items and deliveries received on behalf of the CUSTOMER for suspicious items or tampering.
- 13.5. The CONTRACTOR shall limit access to source code and related design and specification documentation.
- 13.6. The CONTRACTOR shall ensure that there are controls in place to manage the risk of any fraudulent activity in relation to on-line transactions or e-commerce.

**SCHEDULE 2-14**  
**EXIT AND SERVICE TRANSFER ARRANGEMENTS**

**1. INTRODUCTION**

- 1.1. This Schedule 2-14 describes the duties and responsibilities of the CONTRACTOR to the CUSTOMER leading up to and covering the expiry or termination of this Contract and the transfer of service provision to a replacement service provider.
- 1.2. The objectives of the Exit and Service Transfer Arrangements are to ensure a smooth transition of the availability of the Ordered Goods and Ordered Services from the CONTRACTOR to a replacement service provider at the termination or expiry of this Contract.

**2. EXIT AND SERVICE TRANSFER ARRANGEMENTS**

- 2.1. The CONTRACTOR agrees to indemnify and keep the CUSTOMER fully indemnified in respect of any claims, costs, demands, and liabilities arising from the provision of incorrect information provided to the CUSTOMER by the CONTRACTOR, to the extent that any such claim, cost, demand or liability directly and unavoidably arises from the use of the incorrect information in a manner that can reasonably be assumed to be proper in bidding for or providing services similar to the Ordered Goods and Ordered Services.
- 2.2. The CONTRACTOR shall not replace any parts or components of the equipment used for the provision of the Ordered Goods and Ordered Services with parts or components that are of lower quality or which are unsuitable for use in their designed purpose either by a CUSTOMER or a replacement service provider, prior to the expiry date of this Contract or any date of termination hereof.

**3. SERVICES TRANSFER PLAN**

- 3.1. No later than three (3) Months after the execution of this Contract, and thereafter as specified in paragraph 3.3, the CONTRACTOR shall prepare a Services Transfer Plan (STP) for review by the CUSTOMER. The CUSTOMER shall review the STP within twenty (20) Working Days of receipt from the CONTRACTOR and shall notify the CONTRACTOR of any suggested revisions to the STP. In this respect, the CUSTOMER will act neither unreasonably, capriciously nor vexatiously. Such suggested revisions shall be discussed and resolved within ten (10) Working Days. The agreed STP shall be signed as approved by each party.
- 3.2. The STP shall provide comprehensive proposals for the activities and the associated liaison and assistance that will be required for the successful transfer of the Ordered Goods and Ordered Services, including but not limited to the following details:
  - 3.2.1. proposals for the identification and transfer of documentation providing details of the Ordered Goods and Ordered Services;
  - 3.2.2. proposals for the identification of all of the equipment;

- 3.2.3. proposals for the identification of all equipment leases, maintenance agreements and support agreements utilised by the CONTRACTOR in connection with the provision of the Ordered Goods and Ordered Services, together with details of the relevant lessors and contractors, the payment terms, expiry dates and any relevant novation and/or early termination provisions;
- 3.2.4. proposals for the identification and return of all CUSTOMER Furnished Items in the possession of the CONTRACTOR;
- 3.2.5. a detailed summary identifying the owners of title and risk in all the equipment and CUSTOMER Furnished Items following Service Transfer;
- 3.2.6. proposals to enable the CUSTOMER or the replacement service provider to recruit suitably skilled personnel;
- 3.2.7. proposals for the training of key members of the replacement service provider's personnel in connection with the continuation of the provision of the Ordered Goods and Ordered Services following the expiry or termination of this Contract charged at rates agreed between the parties at that time;
- 3.2.8. proposals for the granting of licences to use all software necessary for the CUSTOMER's receipt of the Ordered Goods and Ordered Services and the provision of copies of all related documentation;
- 3.2.9. proposals for the transfer of all CUSTOMER's Data then in the CONTRACTOR's possession to either the CUSTOMER or a replacement service provider, including:
  - 3.2.9.1. an inventory of all CUSTOMER's Data;
  - 3.2.9.2. details of the data structures in which the CUSTOMER's Data is stored, in the form of an agreed data model together with information on other data structures in which the CUSTOMER's Data could be stored;
  - 3.2.9.3. proposed transfer methods, both physical and electronic; and
  - 3.2.9.4. proposed methods for ensuring the integrity of the CUSTOMER's Data on transfer,
- 3.2.10. proposals for providing the CUSTOMER or a replacement service provider copies of:
  - 3.2.10.1. all documentation used in the provision of the Ordered Goods and Ordered Services and necessarily required for the continued use thereof, in which the Intellectual Property Rights are owned by the CONTRACTOR; and
  - 3.2.10.2. all documentation relating to the use and operation of the equipment;
- 3.2.11. proposals for the methods of transfer of the equipment to the CUSTOMER or a replacement service provider;
- 3.2.12. proposals for the assignment or novation of all equipment leases, maintenance agreements and support agreements utilised by the CONTRACTOR in connection with the performance of the Ordered Goods and Ordered Services;

3.2.13. proposals for the disposal of any redundant equipment and materials;  
and

3.2.14. proposals for the supply of any other information or assistance reasonably required by the CUSTOMER or a replacement service provider in order to effect an orderly hand over of the provision of the Ordered Goods and Ordered Services.

3.3. The STP shall be reviewed and updated by the CONTRACTOR. In this regard, the CONTRACTOR shall provide a revised version of the STP to the CUSTOMER on or before 31<sup>st</sup> July and 31<sup>st</sup> January each year, (or more frequently as may be agreed between the parties). The revised STP shall be reviewed and agreed in accordance with the provisions of paragraph 3.1 of this Schedule 2-14.

#### **4. ASSISTANCE ON EXPIRY OR TERMINATION**

4.1. In the event that this Contract expires or is terminated the CONTRACTOR shall, where so requested by the CUSTOMER, provide assistance to the CUSTOMER to migrate the provision of the Ordered Goods and Ordered Services to a replacement service provider including as set out in the Service Transfer Plan.

#### **5. APPLICATION OF TUPE ON A SERVICE TRANSFER**

5.1. The parties acknowledge that a Service Transfer may be a situation to which TUPE and/or the Acquired Rights Directive may apply. In such circumstances, the CUSTOMER or a replacement service provider would inherit liabilities in respect of employees of the CONTRACTOR or any Sub-Contractor engaged in the provision of the Ordered Goods and Ordered Services and, accordingly, the provisions in paragraphs 6 to 8 of this Schedule shall apply.

#### **6. PRE- SERVICE TRANSFER OBLIGATIONS**

6.1. The CONTRACTOR agrees that, subject to compliance with the Data Protection Requirements:

6.1.1. within twenty (20) Working Days of the earliest of:

6.1.1.1. receipt of a notification from the CUSTOMER of a Service Transfer or intended Service Transfer; or

6.1.1.2. receipt of the giving of notice of early termination of this Contract or any part thereof; or

6.1.1.3. the date which is six (6) Months before the due expiry date of this Contract,

6.1.1.4. it shall provide a list of those of its, or its Sub-Contractors', employees which the CONTRACTOR believes will transfer to the CUSTOMER or the replacement service provider (as the case may be), together with details of all relevant terms and conditions of employment, pay, benefits and working arrangements applicable to such employees;

6.1.2. at least ten (10) Working Days prior to the Service Transfer Date, the CONTRACTOR shall provide to the CUSTOMER and any replacement service provider (as the case may be) a final list of employees which shall transfer under TUPE (the “**Transferring Service Provider Employees**”).

6.1.3. subject to compliance with the Data Protection Requirements, the CUSTOMER shall be permitted to use and disclose information provided

by the CONTRACTOR under this paragraph 6 for informing any tenderer or other prospective replacement service provider.

6.2. The CONTRACTOR warrants that the information provided under this paragraph 6 shall be true and accurate.

6.3. From the date of the earliest event referred to in paragraphs 6.1.1.1 to 6.1.1.3 the CONTRACTOR agrees that it shall not, and agrees to procure that its Sub-Contractors shall not, other than in the ordinary course of business, in respect of those employees engaged in the provision of the Ordered Goods and Ordered Services:

6.3.1. increase or reduce the total number of employees so engaged, or give notice to terminate the employment of any such employees; or

6.3.2. replace or re-deploy any such employee other than where any replacement is of equivalent grade, skills, experience and expertise; or

6.3.3. make, propose or permit any changes to their terms and conditions of employment (including any payments connected with the termination of employment).

## **7. TUPE INDEMNITIES**

7.1. The CONTRACTOR shall, and shall procure that any Sub-Contractor shall, perform and discharge all its obligations in respect of all the Transferring Service Provider Employees up to and including the Service Transfer Date. The CONTRACTOR shall indemnify the CUSTOMER and any replacement service provider against all Employee Liabilities arising from the CONTRACTOR's, or any Sub-Contractor's, failure to perform and discharge any such obligation.

7.2. The CONTRACTOR shall indemnify the CUSTOMER and any replacement service provider against any Employee Liabilities in respect of the Transferring Service Provider Employees arising from or as a result of:

7.2.1. any act or omission by the CONTRACTOR or any Sub-Contractor occurring on or before the Service Transfer Date or any other matter, event or circumstance occurring or having its origin before the Service Transfer Date;

7.2.2. any claim made by or in respect of any person employed or formerly employed by the CONTRACTOR or any Sub-Contractor other than a Transferring Service Provider Employee for which it is alleged that the CUSTOMER or any replacement service provider may be liable by virtue of this Contract and/or the Employment Regulations and/or the Acquired Rights Directive; and

7.2.3. any claim made by or in respect of a Transferring Service Provider Employee or any appropriate employee representative (as defined in TUPE) of any Transferring Service Provider Employee relating to any act or omission of the CONTRACTOR or any Sub-Contractor in relation to its or their obligations under Regulation 13 of TUPE except to the extent that the liability arises from the CUSTOMER's or any replacement service provider's failure to comply with Regulation 13(4) of TUPE.

7.3. If any person who is not a Transferring Service Provider Employee claims, or it is determined, that his contract of employment has been transferred from the CONTRACTOR or any Sub-Contractor to the CUSTOMER or any replacement service provider pursuant to TUPE or the Acquired Rights Directive, then:

- 7.3.1. the CUSTOMER or the replacement service provider will, within five (5) Working Days of becoming aware of that fact, give notice in writing to the CONTRACTOR;
- 7.3.2. the CONTRACTOR may offer (or may procure that a Sub-Contractor may offer) employment to such person within fifteen (15) Working Days of the notification by the CUSTOMER or the replacement service provider or take such other steps as it considers appropriate to deal with the matter.
- 7.4. If such offer is accepted, or if the situation has otherwise been resolved by the CONTRACTOR, the CUSTOMER shall and shall use its reasonable endeavours to procure that the replacement service provider shall immediately release the person from his employment.
- 7.5. If, after the fifteen (15) Working Day period specified in paragraph 7.3.2 has elapsed:
- 7.5.1. no such offer of employment has been made; or
- 7.5.2. such offer has been made but not accepted; or
- 7.5.3. , the situation has not otherwise been resolved,
- the CUSTOMER or the replacement service provider may within five (5) Working Days give notice to terminate the employment of such person.
- 7.6. Subject to the CUSTOMER or the replacement service provider acting in accordance with the provisions of this paragraph 7, the CONTRACTOR shall indemnify the CUSTOMER and the replacement service provider against all Employee Liabilities arising out of termination pursuant to the provisions of paragraph 7.5.
- 7.7. If any such person as is described in paragraph 7.3 is neither re-employed by the CONTRACTOR or any Sub-Contractor nor dismissed by the CUSTOMER or replacement service provider within the time scales set out in this paragraph 7, such person will be treated as a Transferring Service Provider Employee.
- 7.8. The CUSTOMER shall, and shall use its reasonable endeavours to procure that the replacement service provider shall indemnify the CONTRACTOR against all Employee Liabilities arising from the CUSTOMER's or a replacement service provider's failure to perform and discharge any obligation and against any Employee Liabilities in respect of the Transferring Service Provider Employee arising from or as a result of any act or omission by the CUSTOMER or a replacement service provider relating to a Transferring Service Provider Employee occurring after the Service Transfer Date or any other matter, event or circumstance occurring or having its origin after the Service Transfer Date.

## **8. THIRD PARTY RIGHTS**

- 8.1. The parties agree that the Contracts (Rights of Third Parties) Act 1999 (CRiTPA) shall apply to paragraph 7 of this Schedule to the extent necessary that any replacement service provider shall have the right to enforce the obligations owed to, and indemnities given to, the replacement service provider by the CONTRACTOR under that paragraph 7 in its own right pursuant to clause 1(1) of CRiTPA.

## **9. PROVISIONS WHERE TUPE DOES NOT APPLY**

- 9.1. If, in the event of a Service Transfer to which TUPE or the Acquired Rights Directive do not apply the following provisions shall apply:

- 9.2. the CUSTOMER or the replacement service provider can, in its discretion, make to any of the employees identified on the list provided by the CONTRACTOR under paragraph 6.1.1 above, an offer, in writing, to employ that employee under a new contract of employment to take effect on the day after the termination referred to in paragraph 9.3 of this Schedule.
- 9.3. When the offer has been made by the CUSTOMER or replacement service provider and accepted by any employee or worker, the CONTRACTOR shall and shall procure that any Sub-Contractor shall permit the employee or worker to leave its employment, as soon as practicable depending on the business needs of the CONTRACTOR, which could be without the employee or worker having worked his full notice period, if the employee so requests.
- 9.4. If the employee does not accept an offer of employment made by the CUSTOMER or replacement service provider, or no such offer is made, the employee shall remain employed by the CONTRACTOR (or the relevant Sub-Contractor, as the case may be) and all Employee Liabilities in relation to the employee shall remain with the CONTRACTOR or the relevant Sub-Contractor and shall indemnify the CUSTOMER and any replacement service provider against any Employment Liabilities that either of them may incur in respect of any such employees of the CONTRACTOR or the relevant Sub-Contractor

## **10. COSTS OF EXIT AND SERVICE TRANSFER ARRANGEMENTS**

- 10.1. The CONTRACTOR will provide resources of sufficient skills and experience to carry out the activities required to fulfil the CONTRACTOR's obligations under this Schedule 2-14 and the Service Transfer Plan. In order to fulfil such obligations the CONTRACTOR shall make full use of staff allocated to the provision of the Ordered Goods and Ordered Services (at no additional cost) and, further, shall provide at no additional cost to the CUSTOMER up to 20 man days of additional resources to carry out any activities which the CONTRACTOR is not ordinarily obliged to provide in the course of the day-to-day provision of the Ordered Goods and Ordered Services (including, without limitation, the establishment and maintenance of the Virtual Library). Any additional resources required by the CUSTOMER from the CONTRACTOR in order for the contractor to fulfil its obligations under this Schedule 2-14 and the Service Transfer Plan shall be provided by the CONTRACTOR upon the request of the CUSTOMER and may be charged in accordance with the Day rates set out in paragraph 5 of schedule 2-3 (The Charges & Charges Variation Procedure).

THIS PAGE HAS BEEN LEFT INTENTIONALLY BLANK

---

**SCHEDULE 2-15**

**BUSINESS CONTINUITY AND DISASTER RECOVERY PROVISIONS**

**1. PURPOSE OF THIS SCHEDULE**

- 1.1. This schedule sets out the CUSTOMER's requirements for ensuring continuity of the business processes and operations supported by the Ordered Goods and Ordered Services in circumstances of Solution disruption or failure and for restoring the Ordered Goods and Ordered Services through business continuity and as necessary disaster recovery procedures. It also includes the requirement on the CONTRACTOR to develop, review, test, change, and maintains a BCDR Plan in respect of the Ordered Goods and Ordered Services and to ensure the CUSTOMER's Business Continuity Plan can be achieved in the event of a disruption to services or a major incident.
- 1.2. The BCDR Plan shall be divided into three parts:
  - 1.2.1. Part A which shall set out general principles applicable to the BCDR Plan ("General Principles").
  - 1.2.2. Part B which shall relate to business continuity ("Business Continuity Plan"); and
  - 1.2.3. Part C which shall relate to disaster recovery ("Disaster Recovery Plan"); and
- 1.3. The BCDR Plan shall detail the processes and arrangements which the CONTRACTOR shall follow to ensure continuity of the business processes and operations supported by the Ordered Goods and Ordered Services following any failure or disruption of any element of the Ordered Goods and Ordered Services and the recovery of the Ordered Goods and Ordered Services in the event of a Disaster.

**2. DEVELOPMENT OF BCDR PLAN**

- 2.1. The CONTRACTOR shall develop a BCDR Plan to be agreed with the CUSTOMER one (1) month before the Service Commencement Date.
- 2.2. The BCDR Plan shall unless otherwise required by the CUSTOMER in writing, be based upon and be consistent with the provisions of paragraphs 3, and 5 of this schedule 2-15 (Business Continuity and Disaster Recovery Provisions).
- 2.3. The CONTRACTOR shall ensure that its Sub-contractors' disaster recovery and business continuity plans are integrated with the BCDR Plan.

**3. PART A - GENERAL PRINCIPLES AND REQUIREMENTS**

- 3.1. The BCDR Plan shall:
  - 3.1.1. set out how the business continuity and disaster recovery elements of the Plan link to each other;
  - 3.1.2. provide details of how the invocation of any element of the BCDR Plan may impact upon the operation of the Ordered Goods and Ordered

Services and any services provided to the CUSTOMER by a Related Service Provider;

- 3.1.3. contain an obligation upon the CONTRACTOR to liaise with the CUSTOMER and (at the CUSTOMER's request) any Related Service Provider with respect to issues concerning business continuity and disaster recovery where applicable;
  - 3.1.4. detail how the BCDR Plan links and interoperates with any overarching and/or connected disaster recovery or business continuity plan of the CUSTOMER and any of its other Related Service Providers as notified to the CONTRACTOR by the CUSTOMER from time to time;
  - 3.1.5. contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multi-channels (including but without limitation a web-site (with FAQs), e-mail, phone and fax) for both portable and desk top configurations, where required by the CUSTOMER;
  - 3.1.6. contain a risk analysis, including:
    - 3.1.6.1. failure or disruption scenarios and assessments and estimates of frequency of occurrence;
    - 3.1.6.2. identification of any single points of failure within the Ordered Goods and Ordered Services and processes for managing the risks arising therefrom;
    - 3.1.6.3. identification of risks arising from the interaction of the Ordered Goods and Ordered Services with the services provided by a Related Service Provider; and
    - 3.1.6.4. a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;
  - 3.1.7. provide for documentation of processes, including business processes, and procedures;
  - 3.1.8. set out key contact details (including roles and responsibilities) for the CONTRACTOR (and any Sub-Contractors) and for the CUSTOMER;
  - 3.1.9. identify the procedures for reverting to "normal service";
  - 3.1.10. set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to ensure that there is no data loss and to preserve data integrity;
  - 3.1.11. identify the responsibilities (if any) that the CUSTOMER has agreed it will assume in the event of the invocation of the BCDR Plan; and
  - 3.1.12. provide for the provision of technical advice and assistance to key contacts at the CUSTOMER as notified by the CUSTOMER from time to time to inform decisions in support of the CUSTOMER's business continuity plans.
- 3.2. The BCDR Plan shall be designed so as to ensure that:
- 3.2.1. the Ordered Goods and Ordered Services are provided in accordance with the Contract at all times during and after the invocation of the BCDR Plan;
  - 3.2.2. the adverse impact of any Disaster, service failure, or disruption on the operations of the CUSTOMER is minimal as far as reasonably possible;

- 3.2.3. it complies with the relevant provisions of ISO/IEC27001 BS 25999 (as amended) and all other industry standards from time to time in force; and
- 3.2.4. there is a process for the management of disaster recovery testing detailed in the BCDR Plan.
- 3.3. The BCDR Plan must be upgradeable and sufficiently flexible to support any changes to the Ordered Goods and Ordered Services or to the business processes facilitated by and the business operations supported by the Ordered Goods and Ordered Services.
- 3.4. The CONTRACTOR shall not be entitled to any relief from its obligations under the Service Levels or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the CONTRACTOR of this Contract.

#### **4. PART B - BUSINESS CONTINUITY ELEMENT - PRINCIPLES AND CONTENTS**

- 4.1. The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes and operations facilitated by the Ordered Goods and Ordered Services remain supported and to ensure continuity of the business operations supported by the Ordered Goods and Ordered Services including but not limited to and unless the CUSTOMER expressly states otherwise in writing:
  - 4.1.1. the alternative processes, (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to the Ordered Goods and Ordered Services; and
  - 4.1.2. the steps to be taken by the CONTRACTOR upon resumption of the Ordered Goods and Ordered Services in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.
- 4.2. The Business Continuity Plan shall address the various possible levels of failures of or disruptions to the Ordered Goods and Ordered Services and the services to be provided and the steps to be taken to remedy to the different levels of failure and disruption. The Business Continuity Plan shall also clearly set out the conditions and/or circumstances under which the Disaster Recovery Plan is invoked.

#### **5. PART C - DISASTER RECOVERY ELEMENT - PRINCIPLES AND CONTENTS**

- 5.1. The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster the CONTRACTOR ensures continuity of the business operations of the CUSTOMER supported by the Ordered Goods and Ordered Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 5.2. The Disaster Recovery Plan shall only be invoked upon the occurrence of a Disaster.
- 5.3. The Disaster Recovery Plan shall include the following:

- 5.3.1. the technical design and build specification of the Disaster Recovery System;
- 5.3.2. details of the procedures and processes to be put in place by the CONTRACTOR and any Sub-contractor in relation to the Disaster Recovery System and the provision of the Disaster Recovery Services and any testing of the same including but not limited to the following:
  - 5.3.2.1. data centre and disaster recovery site audits;
  - 5.3.2.2. backup methodology and details of the CONTRACTOR's approach to data back-up and data verification;
  - 5.3.2.3. identification of all potential disaster scenarios;
  - 5.3.2.4. risk analysis;
  - 5.3.2.5. documentation of processes and procedures;
  - 5.3.2.6. hardware configuration details;
  - 5.3.2.7. network planning including details of all relevant data networks and communication links;
  - 5.3.2.8. invocation rules;
  - 5.3.2.9. Solution recovery procedures;
  - 5.3.2.10. steps to be taken upon Solution resumption to address any prevailing effect of the Solution failure or disruption;
- 5.3.3. any applicable service levels with respect to the provision of Disaster Recovery Services and details of any agreed relaxation upon the Service Levels during any period of invocation of the Disaster Recovery Plan;
- 5.3.4. details of how the CONTRACTOR shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
- 5.3.5. access controls (to any disaster recovery sites used by the CONTRACTOR or any Sub-contractor in relation to its obligations pursuant to this schedule); and
- 5.3.6. testing and management arrangements.

## **6. REVIEW AND AMENDMENT OF THE BCDR PLAN**

- 6.1. The CONTRACTOR shall review part or all of the BCDR Plan (and the risk analysis on which it is based):
  - 6.1.1. on a regular basis and as a minimum once every six calendar months;
  - 6.1.2. following significant changes to the managed service Solution;
  - 6.1.3. within three calendar month of the BCDR Plan (or any part) having been invoked pursuant to paragraph 8 of this schedule; and

- 6.1.4. where the CUSTOMER requests any additional reviews (over and above those provided for in paragraphs 6.1.1 and 6.1.3 of this schedule) by notifying the CONTRACTOR to such effect in writing, whereupon the CONTRACTOR shall conduct such reviews in accordance with the CUSTOMER's written requirements. The costs of both parties for any such additional reviews will be met by the CUSTOMER.
- 6.2. Each review pursuant to paragraph 6.1 of the BCDR Plan shall be a review of the procedures and methodologies set out in the BCDR Plan and shall assess their suitability having regard to any change to the Ordered Goods and Ordered Services or any underlying business processes and operations facilitated by or supported by the Ordered Goods and Ordered Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the CONTRACTOR within the period required by the BCDR Plan or if no such period is required within such period as the CUSTOMER shall reasonably require. The CONTRACTOR shall, within 20 Working Days of the conclusion of each such review of the BCDR Plan, provide to the CUSTOMER a report ("**Review Report**") setting out:
- 6.2.1. the findings of the review;
  - 6.2.2. any changes in the risk profile associated with the Ordered Goods and Ordered Services; and
  - 6.2.3. the CONTRACTOR's proposals ("CONTRACTOR's Proposals") for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan following the review detailing the impact (if any and to the extent that the CONTRACTOR can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any services or systems provided by a third party.
- 6.3. The CONTRACTOR shall as soon as is reasonably practicable after receiving the CUSTOMER's approval of the CONTRACTOR's Proposals (having regard to the significance of any risks highlighted in the Review Report) effect any change in its practices or procedures necessary so as to give effect to the CONTRACTOR's Proposals. Any such change shall be at the CONTRACTOR's expense unless it can be reasonably shown that the changes are required because of a material change to the project's risk profile.

## **7. TESTING OF THE BCDR PLAN**

- 7.1. The CONTRACTOR shall test the BCDR Plan on a regular basis (and in any event not less than [once] in every [Contract Year]). Subject to paragraph 7.2, the CUSTOMER may require the CONTRACTOR to conduct additional tests of some or all aspects of the BCDR Plan at any time where the CUSTOMER considers it necessary, including where there has been any change to the Ordered Goods and Ordered Services or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the BCDR Plan.

- 7.2. If the CUSTOMER requires an additional test of the BCDR Plan it shall give the CONTRACTOR written notice and the CONTRACTOR shall conduct the test in accordance with the CUSTOMER's requirements and the relevant provisions of the BCDR Plan. The CONTRACTOR's costs of the additional test shall be borne by the CUSTOMER unless the BCDR Plan fails the additional test in which case the CONTRACTOR's costs of that failed test shall be borne by the CONTRACTOR.
  - 7.3. Following each test, the CONTRACTOR shall send to the CUSTOMER a written report summarising the results of the test and shall promptly implement any actions or remedial measures which the CUSTOMER considers to be necessary as a result of those tests.
  - 7.4. The CONTRACTOR shall undertake and manage testing of the BCDR Plan in full consultation with the CUSTOMER and shall liaise with the CUSTOMER in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the CUSTOMER in this regard. Each test shall be carried out under the supervision of the CUSTOMER or its nominee.
  - 7.5. The CONTRACTOR shall ensure that any use by it or any Sub-contractor of "live" data in such testing is first approved with the CUSTOMER. Copies of live test data used in any such testing shall be (if so required by the CUSTOMER) destroyed or returned to the CUSTOMER on completion of the test.
  - 7.6. The CONTRACTOR shall, within [20 Working Days] of the conclusion of each test, provide to the CUSTOMER a report setting out:
    - 7.6.1. the outcome of the test;
    - 7.6.2. any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and
    - 7.6.3. the CONTRACTOR's proposals for remedying any such failures with times for resolution for agreement with the CUSTOMER.
  - 7.7. Following each test, the CONTRACTOR shall take all measures requested by the CUSTOMER, (including requests for the re-testing of the BCDR Plan) to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the CONTRACTOR, at no additional cost to the CUSTOMER, by the date reasonably required by the CUSTOMER and set out in such notice.
  - 7.8. For the avoidance of doubt, the carrying out of a test of the BCDR Plan (including a test of the BCDR Plan's procedures) shall not relieve the CONTRACTOR of any of its obligations under this schedule 8.6 or otherwise.
  - 7.9. The CONTRACTOR shall also perform a test of the BCDR Plan as part of the commissioning of any new project.
- 8. INVOCATION OF THE BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN**

- 8.1. In the event of a complete loss of service or in the event of a Disaster, the CONTRACTOR shall immediately invoke the BCDR Plan (and shall inform the CUSTOMER promptly of such invocation). In all other instances the CONTRACTOR shall only invoke or test the BCDR Plan with the prior consent of the CUSTOMER.

**9. PART C - DISASTER RECOVERY ELEMENT - PRINCIPLES AND CONTENTS**

- 9.1. The CONTRACTOR shall provide contingency planning and disaster recovery management for systems, to agreed service levels
- 9.2. The CONTRACTOR shall provide named representative to take responsibility for disaster recovery management and business continuity planning.
- 9.3. The CONTRACTOR shall ensure that managed service Solution continuity plans, contact lists and the Configuration Management Library (and all resources required to effect recovery) are available when normal office access is prevented.
- 9.4. The CONTRACTOR shall allow CUSTOMER or those instructed by CUSTOMER to complete an audit of the CONTRACTOR's managed service continuity plan.