North Ayrshire Council
Comhairle Siorrachd Àir a Tuath

North Ayrshire Council Terms and Conditions 5 (NAC TC5) Conditions of Contract for Information Communication Technology (ICT) Services

These conditions may only be varied with the written agreement of the Purchaser. No terms or conditions put forward at any time by the Supplier shall form any part of the contract unless specifically agreed in writing by the Purchaser.

Contents

1. Definitions

In these conditions:

“Affiliate” means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;

“Baseline Security Requirements” means the schedule which provides the baseline mandatory security requirements for all Suppliers;

“BCDR Plan” means any plan prepared pursuant to paragraph 1 of Schedule 3 (Business Continuity and Disaster Recovery), as may be amended from time to time;

“Breaches of Security” means the occurrence of:

(a) any unauthorised access to or use of the Services, the Purchaser’s premises, the Premises, the Supplier’s System, the Purchaser’s System (to the extent that it is under the control of the Supplier) and/or any IT, information or data (including the Confidential Information and the Purchaser Data) used by the Purchaser and/or the Supplier in connection with this Contract; and/or

(b) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Purchaser Data), including any copies of such information or data, used by the Purchaser and/or the Supplier in connection with this Contract, in either case as more particularly set out in the security requirements in the Service Specification; and/or

(c) a Cyber Security Incident.

“Business Continuity Plan” has the meaning given in paragraph 1.2.1(b) of Schedule 3 (Business Continuity and Disaster Recovery)

“Business Continuity Services” has the meaning given in paragraph 3.2.2 of Schedule 3 (Business Continuity and Disaster Recovery);

“CHECK Scheme” means the scheme for penetration testing of data processing systems operated by the National Cyber Security Centre;

"Confidential Information" means any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information the disclosure of which would, or would be likely to, prejudice the commercial interests of any person, trade secrets, Intellectual Property Rights and know-how of either Party and all Personal Data;

“Contract” means any formal Contract entered into between the Supplier and North Ayrshire Council. The documents that form part of the Contract include, but are not limited to, the invitation to quote/tender (including any and all associated schedules), any clarification sought as part of the procurement process, these terms and conditions and the award letter;

“Contract Administrator” means the member of the Purchasers staff appointed for the purposes of overseeing the Contract, monitoring the performance of the Supplier and ensuring that the standards of service specified in the Contract are delivered. The Contract Administrator and their deputy shall be named at contract award;

“Control” means the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;

“COTS Software” means Supplier Software and Third Party Software (including open source software) that the Supplier makes generally available commercially prior to the date of signature of this Contract (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price;

“Cyber Security Incident” means anything, event, act or omission which gives, or may give, rise to:

(a) unauthorised access to any information system, data or electronic communications network (including breach of an applicable security policy);

(b) reduced integrity of an information system, data or electronic communications network;

(c) unauthorised use of any information system or electronic communications network for the processing (including storing) of data;

(d) disruption or change of the operation (including, but not limited to, takeover of control, malicious disruption and/or denial of service) of an information system or electronic communications network;

(e) unauthorised changes to firmware, software or hardware;

(f) unauthorised destruction, damage, deletion or alteration of data residing in an information system or electronic communications network;

(g) removal or limiting the availability of, or possibility to use, data residing in an information system or electronic communications network;

(h) the appropriation, publication, dissemination or any other use of data by persons unauthorised to do so; or

(i) a breach of the Computer Misuse Act 1990, the Network and Information Systems Regulations 2018, the Data Protection Laws, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Communications Act 2003, the Official Secrets Act 1911 to 1989, or any other applicable legal requirements in connection with cybersecurity and/or privacy

in connection with the Services and/or this Contract.

“Data Breach**”** means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier or any sub-contractor under or in connection with the Contract, and/or actual or potential loss and/or destruction and/or corruption of Personal Data in breach of the Contract, including but not limited to any Personal Data Breach;

“Data Controller” has the meaning given in the Data Protection Laws;

“Data Processor” has the meaning given in the Data Protection Laws;

“Data Protection Laws” means any law, statute, subordinate legislation regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body which relates to the protection of individuals with regard to the processing of Personal Data to which a Party is subject including the Data Protection Act 2018 and any statutory modification or re-enactment thereof and the UK GDPR;

“Data Subject” has the meaning given in the Data Protection Laws;

“Detailed Implementation Plan” means the plan developed and revised from time to time;

“Disaster” means the occurrence of one or more events which, either separately or cumulatively, mean, in the opinion of the Purchaser, that the Services, or a material part of the Services will not be available and significant effort is required to restore the Services;

“Disaster Recovery Plan” has the meaning given in paragraph 1.2.1(c) of Schedule 3 (Business Continuity and Disaster Recovery);

“Disaster Recovery Services” means the services embodied in the processes and procedures for restoring the Services following the occurrence of a Disaster;

“Disaster Recovery System” means the system used for the purpose of delivering the Disaster Recovery Services;

“Equipment” means equipment, plant, tackle, materials and other items supplied and used by the Supplier’s Representatives in the performance of the Supplier’s obligations under this Contract;

“Good Industry Practice” means standards, practices, methods and procedures conforming to legal and regulatory requirements and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking as the Supplier under the same or similar circumstances;

“Government Body” means a body listed in one of the following sub-categories of the Scottish Government’s National Public Bodies Directory, as published and amended from time to time:

(a) Scottish Government Department;

(b) Non-Departmental Public Body (advisory, executive, or tribunal);

(c) Non-Ministerial Department;

(d) Other government funded organisation;

(e) Any Contracting Authority; or

(f) Executive Agency.

“Intellectual Property Rights” means all copyright, patent, trademark, design right, database right and any other right in the nature of intellectual property whether or not registered, in any materials or works in whatever form (including but not limited to any materials stored in or made available by means of an information technology system and the computer software relating thereto) which are created, produced or developed as part of the Services by or on behalf of the Supplier;

“IT Environment” means the Purchaser System and the Supplier System;

“Key Performance Indicators” means the performance measures detailed within the Contract which the Supplier must adhere to;

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

“Open Source Software” means computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other Intellectual Property Rights in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge

“Party” means the Supplier and Purchaser respectively;

“Parties” means the Supplier and Purchaser collectively;

“Personal Data” has the meaning given in the Data Protection Laws;

“Personal Data Breach” has the meaning given in the Data Protection Laws;

“Premises” means the location where the Services are to be performed, as specified in the Contract;

“Processing” has the meaning given in the Data Protection Laws and cognate expressions shall be construed accordingly;

“Procurement Card” means a type of company charge card used for smaller purchases to achieve greater cost efficiency, control and convenience. Procurement cards are also known as Purchasing Cards, P-Cards or PCards;

“Purchase Order” means the document setting out the Purchaser's requirements for the Contract;

“Purchaser” means North Ayrshire Council;

“Purchaser Data” means the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:

(a) supplied to the Supplier by or on behalf of the Purchaser; and/or

(a) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or

(b) any Personal Data for which the Purchaser is the Data Controller;

“Purchaser Property” means any corporeal moveable property issued or made available to the Supplier by the Purchaser in connection with this Contract;

“Purchaser’s Protected Information” means any information of a confidential nature or business data obtained by the Supplier by reason of this Contract except information which is in the public domain otherwise than by reason of a breach of this Contract;

“Purchaser’s System” means the Purchaser's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Purchaser or the Supplier in connection with this Contract which is owned by the Purchaser or licensed to it by a third party and which interfaces with the Supplier’s System or which is necessary for the Purchaser to receive the Services;

“Related Supplier” means any person who provides services to the Purchaser in relation to this Contract from time to time;

“Security Plan” means the security management system, plan and processes to be developed by the Supplier (including areas such as policy, staff management, supply chain management, asset management, technical controls and software life cycle management to ISO 27001 or equivalent) in accordance with paragraph **Error! Reference source not found.** of Schedule 2 (Security Management) as updated from time to time in accordance with this Contract;

“Service Specification” means the document forming part of the procurement process which sets out the Purchaser’s requirements and objectives of each stage of the delivery of the Services;

“Services” means the Services to be provided as specified in the Purchase Order and shall, where the context so admits, include any materials, articles and goods to be supplied, assigned thereunder;

“Software” means Specially Written Software, Supplier Software and Third Party Software;

“Sub-Contract” means a Contract between two or more Suppliers, at any stage of remoteness from the Purchaser in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Contract;

“Supervisory Authority” has the meaning given in the Data Protection Laws;

“Supplier” means the person, firm or company to whom the Contract is issued;

“Supplier Representative” or “Supplier Representatives” or “Supplier’s Representatives” means all persons engaged by the Supplier in the performance of its obligations under the Contract including but not limited to:

- its Staff
- its agents, suppliers and carriers; and
- any sub-contractors of the Supplier (whether approved under Condition 21 (Assignation and Sub-Contracting) or otherwise).

“Supplier Software” means software which is proprietary to the Supplier (or an Affiliate of the Supplier) and which is or will be used by the Supplier for the purposes of providing the Services;

“Supplier’s System” means the information and communications technology system used by the Supplier in implementing and performing the Services including the Software, the Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Purchaser’s System);

“Staff” means any persons employed by the Supplier, and any persons employed by a third party but working for and under the control of the Supplier, who are or may be at any time concerned with the Services or any part of them;

“Third Party Software” means software which is proprietary to any third party (other than an Affiliate of the Supplier) or any Open Source Software which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services;

“Working Day” or “Working Days” means a day on which the Purchaser is open to the general public; and

“UK GDPR” means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data as it forms part of the law of the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and 2020.

2. Modification of Contract

2.1 The Purchaser may order any modification to any part of the Services that for any other reason shall in the Purchaser's opinion be desirable. Any such modification will be made in accordance with this Condition 2, and shall include but not be limited to the following:

2.1.1 To perform additional Services, as the Purchaser may require;

2.1.2 To omit or to cease to perform the Services or any part thereof for such period as the Purchaser may require;

2.1.3 To make alterations and substitutions to the Service Specification, and to perform the Services in accordance with the Service Specification as so modified;

2.1.4 To make changes in quality, form, character, kind, timing, method or sequence of the Services.

2.2 Where the Purchaser is considering a modification to the Services, it shall notify the Supplier in writing. Within the timescale stipulated by the Purchaser in said notification, the Supplier shall confirm in writing the effect, if any, the modification shall have on the Contract, including any effect on prices. Where an omission, addition or modification of the Services will result in additional costs to the Purchaser (as can be reasonably demonstrated by the Supplier to the Purchaser) or a saving to the Purchaser, such sum shall be agreed between the Parties in advance. Failing such agreement, the Purchaser (acting reasonably) shall be entitled to determine the appropriate sum attributable to the modification and shall notify the Supplier accordingly.

2.3 The Purchaser shall confirm the proposed modification by issuing a modification letter to the Supplier. Immediately upon receipt of the modification letter from the Purchaser the Supplier shall be bound by, and shall forthwith carry out, the terms of that letter.

3. Inspection of the Supplier's Premises and Documentation

3.1 Following award of the Contract, the Supplier shall permit representatives of the Purchaser, following the giving of reasonable notice, except in cases of urgency, to have access to the Premises, to inspect the Premises, to ensure that they are fit for the purposes of the Contract, that they comply with the conditions of the Contract, all applicable law, Good Industry Practice, and to permit the representatives to carry out external quality audits and assessments of the Supplier.

3.2 Separately, the Supplier is obliged throughout the duration of the Contract to make available on request to the Purchaser all available documentation to substantiate its compliance with the conditions of the Contract, all applicable law and Good Industry Practice, or any other requirements of the Contract relating to quality assurance and assessment of the Supplier's performance of its obligations under the Contract.

3.3 Any breach of this Condition 3 by the Supplier is a material breach for the purposes of Condition 19.2 (Termination).

4. Security and Access to the Purchaser's Premises

4.1 Any access to, or occupation of, the Purchaser's premises which the Purchaser may grant the Supplier from time to time is on a non-exclusive licence basis free of charge. The Supplier must use the Purchaser's premises solely for the purpose of performing its obligations under the Contract and must limit access to the Purchaser's premises to such individuals as are necessary for that purpose.

4.2 The Supplier must comply with the Purchaser's controls, procedures and policies concerning security and access to the relevant Purchasers premises and any such modifications to those controls, procedures and policies or replacement controls, procedures and policies as are notified to the Supplier from time to time.

4.3 The Supplier must notify the Purchaser of any matter or other change in circumstances which might adversely affect future security and access to the Purchasers premises.

4.4 At the Purchaser's written request, the Supplier must provide a list of the names and addresses of all persons who may require admission to the Purchaser's premises in connection with the Contract, specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Purchaser may reasonably request.

4.5 The Supplier must ensure that any individual Supplier Representative entering the Purchaser's premises complies with any controls, procedures and policies, if applicable, for obtaining access. The Supplier acknowledges that the Purchaser has the right to deny entry to any individual that does not comply with the Purchaser's controls, procedures, and policies concerning security and access

4.6 In accordance with the Purchaser's controls, procedures and policies concerning visitor access, entry to the Purchaser's premises may be granted to individual Supplier Representatives for the purposes of meetings.

4.7 The Purchaser may, by notice to the Supplier, refuse to admit onto, or withdraw permission to remain on, the Purchaser's premises any Supplier Representative whose admission or continued presence would, in the opinion of the Purchaser acting reasonably, be undesirable.

4.8 The Purchaser will provide advice and assistance acting reasonably to the Supplier to facilitate the Supplier's compliance with this Condition 4.

4.9 All decisions of the Purchaser under this Condition are final and conclusive.

4.10 Breach of this Condition 4 by the Supplier is a material breach for the purposes of Condition 19.2 (Termination).

5. Supplier's Status

5.1 In carrying out the Services the Supplier shall be acting as principal and not as the agent of the Purchaser. Accordingly:

(a) the Supplier shall not (and shall procure that any Supplier Representatives do not) say or do anything that might lead any other person to believe that the Supplier is acting as the agent of the Purchaser or do anything that might lead to the Purchaser's name being held in disrepute or lead any other person to do so, and

(b) nothing in this Contract shall impose any liability on the Purchaser in respect of any liability incurred by the Supplier to any other person but this shall not be taken to exclude or limit any liability of the Purchaser to the Supplier that may arise by virtue of either a breach of this Contract or any negligence on the part of the Purchaser, or the Purchaser's staff or agents.

6. Supplier's Personnel

6.1 The Supplier shall provide full particulars as required by the Purchaser of all Supplier Representatives, including but not limited to, a list of names and addresses of Supplier Representatives, specifying the capacities in which they are so concerned with the Services and the performance of the Contract. The Supplier shall take all reasonable steps to avoid changes of Supplier Representatives performing the Contract and shall provide the Purchaser with one (1) month's written notice and full particulars of any proposed additional or replacement Supplier Representatives.

6.2 At any time, the Purchaser may give notice to the Supplier that any Supplier Representatives are not to become or be involved further with the performance of the Contract, and may require the Supplier to replace any Supplier Representatives removed under this Condition with another suitably qualified person. The decision of the Purchaser regarding the Supplier Representatives shall be final and conclusive. The Supplier shall act immediately on receipt of such notice to comply with the notice, including but not limited to, taking all necessary steps to avoid unauthorised person(s) from gaining access to the Premises and the Purchaser's premises.

6.3 The Supplier shall bear the cost of any notice, instruction or decision of the Purchaser under this Condition 6.

7. Manner of Carrying out the Services

7.1 The Supplier shall make no delivery of materials, plant or other items nor commence any Services on the Premises without obtaining the Purchaser's prior consent.

7.2 Access to the Premises shall not be exclusive to the Supplier but only such as shall enable the Supplier to carry out the Services concurrently with the execution of Works/Services by others. The Supplier shall co-operate with such others as the Purchaser may reasonably require.

7.3 The Purchaser shall have the power at any time during the progress of the Services to order in writing:

(a) the removal from the Premises of any materials which in the sole opinion of the Purchaser are either hazardous, noxious or not in accordance with the Contract, and/or

(b) the substitution of proper and suitable materials, and/or

(c) the removal and proper re-execution notwithstanding any previous test thereof or interim payment therefor of any Services which, in respect of material or workmanship is not in the sole opinion of the Purchaser in accordance with the Contract.

7.4 The Supplier shall immediately comply with any order made under Condition 7.3.

7.5 On completion of the Services the Supplier shall remove the Supplier's plant, equipment and unused materials and shall clear away from the Premises all rubbish arising out of the Services and leave the Premises in a neat and tidy condition.

8. Health and Safety

8.1 The Supplier shall perform the Services in such a manner as to be safe and without risk to the health or safety of persons in the vicinity of the place where the Services are being performed (whether such persons are in the vicinity of the said place at the time when the Services are being performed or otherwise) and in such a manner as to comply with any relevant health and safety or other legislation (including Statutory Instrument, Orders, or Regulations made under the said legislation) and any requirements imposed by a local or other regulatory authority in connection with the performance of Services of the type supplied to the Purchaser, whether specifically or generally. The Supplier shall indemnify the Purchaser against all actions, suits, claims, demands, losses, charges, costs and expenses which the Purchaser may suffer or incur as a result of or in connection with any breach of this Condition.

8.2. The Supplier must notify the Purchaser immediately of any risks to health or safety which are identified or arise during the Contract including, but not limited to, any known misuse or abuse of any Services provided.

8.3. Notwithstanding Condition 4 (Security and Access to the Purchaser's Premises) of this Contract the Supplier shall comply with any health and safety measures implemented by the Purchaser in respect of the Purchaser's premises when accessing and/or occupying the Purchaser's premises, and shall notify the Purchaser immediately of any incident(s) which causes or is likely to cause any personal injury or damage to property when accessing and/or occupying the Purchaser's premises.

8.4. The Supplier shall notify the Purchaser immediately of any health and safety hazards which may exist or arise at the Premises which may affect the Supplier's performance of its duties under the Contract.

8.5 The Supplier shall ensure that its health and safety policy statement (as required by The Health and Safety at Work etc. Act 1974) is made available to the Purchaser on request.

9. Time of Performance

9.1 Time is of the essence in the performance of this Contract.

9.2 The Supplier shall begin performing the Services on the date stated in the Purchase Order and shall complete the Services by the date stated in the Purchase Order or continue to perform them for the period stated in the Purchase Order (whichever is applicable). The Purchaser may by written notice require the Supplier to execute the Services in such order as the Purchaser may decide. In the absence of such notice the Supplier shall submit such detailed programmes of work and progress reports as the Purchaser may from time to time require.

10. Payment

10.1 Unless otherwise stated in the Contract, payment will be made within thirty (30) days of receipt and agreement of invoices, submitted monthly in arrears, for Services completed to the satisfaction of the Purchaser.

10.2 The Purchaser will not be liable to pay for any Services carried out by the Supplier unless it is specified in a Purchase Order.

10.3 Value Added Tax, where applicable, shall be shown separately on all invoices as a strictly net extra charge.

10.4 The Supplier shall be obliged to accept payment by means of BACS (Banks Automated Clearing Service) or Procurement Card.

11. Free-Issue Materials

11.1 Where the Purchaser for the purpose of the Contract issues materials free of charge to the Supplier such materials shall be and remain the property of the Purchaser. The Supplier shall maintain all such materials in good order and condition and shall use such materials solely in connection with the Contract. The Supplier shall notify the Purchaser of any surplus materials remaining after completion of the Services and shall dispose of them as the Purchaser may direct. Waste of such materials arising from bad workmanship or negligence of the Supplier or any of the Supplier's Representatives shall be made good at the Supplier's expense. Without prejudice to any other rights of the Purchaser, the Supplier shall deliver up such materials whether processed or not to the Purchaser on demand.

12. Audit

12.1 The Supplier shall keep and maintain until the date falling seven (7) years after the date of expiry of the Contract or any period of extension, or as long a period as may be agreed between the parties, full and accurate records of the Contract including the Services supplied under it, all expenditure reimbursed by the Purchaser, and all payments made by the Purchaser. The Supplier shall on

request afford the Purchaser such access to those records as may be requested by the Purchaser in connection with the Contract.

12.2 The provisions of this Condition 12 shall apply during the continuance of this Contract and after its termination howsoever arising.

13. Corrupt Gifts or Payments

13.1 The Supplier shall not offer or give, or agree to give, to any employee or representative of the Purchaser any gift or consideration of any kind as an inducement or reward for doing or refraining from doing or for having done or refrained from doing, any act in relation to the obtaining or execution of this or any other Contract with the Purchaser or for showing or refraining from showing favour or disfavour to any person in relation to this or any such Contract. The attention of the Supplier is drawn to the criminal offences created by the Bribery Act 2010.

14. Intellectual Property Rights

14.1 All Intellectual Property Rights in any material including but not limited to reports, guidance, specification, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs which are created or developed by the Supplier on behalf of the Purchaser for use, or intended use, in relation to the performance by the Supplier of its obligations under the Contract are hereby assigned to and shall vest in the Purchaser absolutely.

14.2 Any material, including but not limited to reports, guidance, specification, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs, furnished to or made available to the Supplier by or as directed by the Purchaser shall remain the property of the Purchaser.

14.3 Except as may expressly be provided for in the Contract, neither Party acquires any interest in or license to use the other Party's Intellectual Property Rights owned or developed prior to or independently of the Contract.

14.4 The Supplier must not infringe any Intellectual Property Rights of any third party in providing the Services or otherwise performing its obligations under the Contract. The Supplier shall indemnify the Purchaser against all actions, claims, demands, losses, charges, costs and expenses which the Purchaser may suffer or incur as a result of or in connection with any breach of this Condition 14.4.

14.5 The Supplier shall, at the request of the Purchaser, provide the Purchaser with a complete and up-to-date copy of all electronically stored data and all other information necessary to ensure that the Purchaser can continue to use the electronically stored data so provided by the Supplier; all to the reasonable satisfaction of the Purchaser.

14.6 Electronically stored data shall mean data however stored on a computer storage medium, and shall include data stored in conventional files, databases and computer aided design files, and which contain relevant design information. The Supplier shall store all data on a suitable medium in either its native format or in a neutral file format to suit the Purchasers requirements.

14.7 The Purchaser reserves the right to verify and validate any information contained within the electronically stored data within one (1) year from completion of the Services. The Supplier shall remedy at their own expense any defects or inadequacies discovered during the said one (1) year and notified by the Purchaser to the Supplier and such defects or inadequacies shall be remedied within fourteen (14) Working Days of receipt of such notification.

14.8 The Supplier shall not have the right to use any reports, or other materials referred to in Condition 14.1 without the prior written consent of the Purchaser and then only upon such terms as may be imposed in connection therewith, except for information which is in the public domain.

14.9 The provisions of this Condition shall apply during the continuance of this Contract and after its termination howsoever arising.

15. Indemnity and Insurance

15.1 Without prejudice to any rights or remedies of the Purchaser, the Supplier shall indemnify the Purchaser against all actions, suits, claims, demands, losses, charges, costs and expenses which the Purchaser may suffer or incur as a result of or in connection with any damage to property or in respect of any injury (whether fatal or otherwise) to any person which may result directly or indirectly from any negligent or wrongful act or omission of the Supplier.

15.2 Except in the case of loss, damage or personal injury (including death) suffered by an employee of the Supplier (in respect of which the indemnity in Condition 15.1 shall apply whether or not the loss, damage or personal injury was caused by the negligent or wilful act or omission of the Purchaser or any agent) the indemnity contained in Condition 15.1 shall not apply to the extent that the loss, damage or injury is caused by the negligent or wilful act or omission of the Purchaser.

15.3 The Purchaser shall indemnify the Supplier in respect of all claims, proceedings, actions, damages, fines, costs, expenses or other liabilities which may arise out of, or in consequence of, a breach of Data Protection Laws where the Supplier has acted in accordance with the Purchaser's written instructions, notwithstanding the above, nothing within this Contract relieves the Supplier of any of their own direct responsibilities and liabilities under Data Protection Laws.

15.4 The Supplier shall have in force and shall require any Sub-Contractor to have in force:

(a) Employer's liability insurance, to the value of at least ten million pounds (£10,000,000) sterling in respect of any one event and unlimited in the period, for the duration of the Contract, unless exempt under the Employers' Liability (Compulsory Insurance) Act 1969.

(b) Public liability insurance, to the value of at least ten million pounds (£10,000,000) sterling in respect of any one event and unlimited in the period, for the duration of the Contract.

(c) Professional indemnity insurance, to the value of at least five million pounds (£5,000,000) sterling in the aggregate in the policy period, for the duration of the Contract, plus a period of six (6) years following completion of the whole of the Services or earlier termination.

(d) Cyber liability insurance, to the value of at least five million pounds (£5,000,000) sterling in respect of any one event and unlimited in the period for the duration of the Contract.

(e) Third-party motor vehicle insurance maintained throughout the period of the Contract, in accord with the provisions of the current Road Traffic Act 1988 (as amended). A valid motor vehicle certificate in the Supplier's name, or (where there is no fleet but rather the Supplier permits employees to use their personal vehicles for business purposes), a letter signed by a person of appropriate authority, confirming that the Supplier has ongoing arrangements in place to ensure their employees' vehicles are appropriately insured and maintained.

15.5 The policy or policies of insurance referred to in Condition 15.4 shall be shown to the Purchaser whenever the Purchaser requests, together with satisfactory evidence of payment of premiums, including the latest premium due thereunder.

15.6 The Supplier shall establish a robust internal process to receive and process any insurance claims intimated to it, the detail of which process will be made available to the Purchaser on request.

15.7 In the event that a claim is intimated to the Supplier, the Supplier shall immediately acknowledge receipt of such claim to the claimant, investigate the facts and process the claim with its insurance company to the Purchaser's satisfaction. If required by the Purchaser, the Supplier shall provide any information required on the nature of the claim or the manner in which it is being processed, having in mind that the Purchaser's name cannot be brought into disrepute.

16. Equality

16.1 The Supplier undertakes that it has and shall comply with all statutory requirements in respect of ensuring equal opportunity in employment and has not and shall not unlawfully discriminate either directly or indirectly on such grounds as race, colour, ethnic or national origin, disability, gender, sex or sexual orientation, religion or belief, or age and without prejudice to the generality of the foregoing the Supplier shall not unlawfully discriminate within the meaning and scope of the Equality Acts 2006 and 2010, the Part-Time Workers (Prevention of Less Favourable Treatment) Regulations 2000, the Fixed-Term Employees (Prevention of Less Favourable Treatment) Regulations 2002, the Human Rights Act 1998 or other relevant or equivalent legislation, and any statutory modification or re-enactment thereof. The Supplier shall take all reasonable steps to secure the observance of this Condition 16 by all employees and representatives of the Supplier.

17. Blacklisting

17.1 The Supplier must not commit any breach of the Employment Relations Act 1999 (Blacklists) Regulations 2010 or section 137 of the Trade Union and Labour Relations (Consolidation) Act 1992. Breach of this Condition is a material default which shall entitle the Purchaser to terminate the Contract.

17.2 Suppliers sub-contracting, assigning or novating any part of the Contract must impose the same conditions on any sub-contractor or party to whom such a part of the Contract is novated or assigned.

18. Confidentiality

18.1 The Supplier shall keep secret and not disclose and shall procure that the Supplier's Representatives keep secret and do not disclose any information of a confidential nature or business data obtained by the Supplier by reason of this Contract except information which is in the public domain otherwise than by reason of a breach of this Condition.

18.2 All information related to the Contract will be treated as commercial in confidence by the parties except that the Supplier or Purchaser or both may disclose any information as required by law or judicial order to be disclosed.

18.3 The Supplier shall at all times comply with the Purchaser's "IT and Cyber Security Policy" ("the Policy") and it is the Supplier's responsibility to ensure that the Supplier and the Supplier's Representatives are familiar with and comply with the Policy as well as with any of the Purchaser's related security standards, guidelines and procedures in relation to the Policy. The Policy can be obtained on request by contacting the Purchaser's ICT Security Team by email at cybersecurityteam@north-ayrshire.gov.uk.

18.4 The provisions of this Condition 18 shall apply during the continuance of this Contract and after its termination howsoever arising.

19. Termination

19.1 The Supplier shall notify the Purchaser in writing immediately upon the occurrence of any of the following events:

(a) where the Supplier is an individual and if a petition is presented for the Supplier's bankruptcy or the sequestration of the Supplier's estate or a criminal bankruptcy order is made against the Supplier, or the Supplier is apparently insolvent, or makes any composition or arrangement with or for the benefit of creditors, or makes any conveyance or assignation for the benefit of creditors, or if an administrator or trustee is appointed to manage the Supplier's affairs; or

(b) where the Supplier is not an individual but is a firm, or a number of persons acting together in any capacity, if any event in (a) or (c) of this Condition occurs in respect of the firm or any partner in the firm or any of those persons or a petition is presented for the Supplier to be wound up as an unregistered company; or

(c) where the Supplier is a company, if the company passes a resolution for winding-up of dissolution (otherwise than for the purposes of and followed by an amalgamation or reconstruction) or the court makes an administration order or a winding-up order, or the company makes a composition or arrangement with its creditors, or an administrator, administrative receiver, receiver or manager is appointed by a creditor or by the court, or possession is taken of any of its property under the terms of a floating charge.

19.2 On the occurrence of any of the events described in Condition 19.1 or, if the Supplier shall have committed a material breach of this Contract and (if such breach is capable of remedy) shall have failed to remedy such breach within thirty (30) days of being required by the Purchaser in writing to do so or, where the Supplier is an individual if the Supplier shall die or be adjudged incapable of managing his or her affairs within the meaning of the Adults with Incapacity (Scotland) Act 2000 or the Mental Health (Care and Treatment) (Scotland) Act 2003, the Purchaser shall be entitled to terminate this Contract by notice to the Supplier with immediate effect, or at such later date as the Purchaser may specify. Thereupon, without prejudice to any other of the Purchaser's rights, the Purchaser may complete the Services or have them completed by a third party, using for that purpose (making a fair and proper allowance therefor in any payment subsequently made to the Supplier) all materials, plant and equipment on the Premises belonging to the Supplier, and the Purchaser shall not be liable to make any further payment to the Supplier until the Services have been completed in accordance with the requirements of the Contract, and shall be entitled to deduct from any amount due to the Supplier the costs thereof incurred by the Purchaser (including the Purchaser's own costs). If the total cost to the Purchaser exceeds the amount (if any) due to the Supplier, the difference shall be recoverable by the Purchaser from the Supplier.

19.3 Notwithstanding Conditions 19.1 and 19.2 and without prejudice to any other rights the Purchaser may have under the Contract or otherwise in law, the Purchaser shall be entitled to terminate the Contract immediately (or at such later date as the Purchaser may specify) by notice in writing to the Supplier, in the event that:

(a) the Contract has been subject to substantial modification which would have required a new procurement procedure in accordance with regulation 72(9) (modification of contracts during their term) of The Public Contracts (Scotland) Regulations 2015; or

(b) the Supplier has at the time of contract award, been in one of the situations referred to in regulation 58(1) (exclusion grounds) of The Public Contracts (Scotland) Regulations 2015, including as a result of the application of regulation 58(2) of those regulations, and should therefore have been excluded from the procurement procedure; or

(c) the Contract should not have been awarded to the Supplier in view of a serious infringement of the Purchaser's obligations under The Public Contracts (Scotland) Regulations 2015 as amended by The Public Procurement etc. (Scotland) Amendment (EU Exit) Regulations 2020, Directive 2014/24/EU of the European Parliament, and any statutory modifications thereof; or

(d) the Supplier fails to provide or complete delivery of the Services or any portion thereof within the timescales specified in the Contract or where not so specified in the Purchase Order; or

(e) the Supplier fails to deliver the Services or any portion thereof in accordance with the Key Performance Indicators, and if such failure is capable of remedy the Supplier fails to remedy such failure within thirty (30) days of being required by the Purchaser in writing to do so; or

(f) the Supplier suspends performance of the Services or commits any other act from which an intention to abandon the Contract can be reasonably inferred, of which the Purchaser shall be the sole judge; or

(g) the Supplier fails to comply in the performance of the Services with any legal obligations and requirements under all applicable law, including without restriction: environmental law, social law, employment law, the Health and Safety at Work etc. Act 1974, and the Equality Act 2010; or

(h) the Supplier operates the Services without insurance cover as required under Condition15 (Indemnity and Insurance); or

(i) the Supplier fails to supply information required by the Purchaser in terms of Condition 10 (Payment); or

(j) the Supplier, or any person employed by the Supplier or acting on behalf of the Supplier (whether with or without the knowledge of the Supplier), having offered, paid or given, directly or indirectly, any gift in money or in any other form to any member, employee or agent of the Purchaser as an inducement or reward for doing or forbearing to do or for having forborne to do any action in relation to the obtaining or execution of the Contract or any other contract with the Purchaser or for showing or forbearing to show favour or disfavour to any person in relation to the Contract or any other contract with the Purchaser, or in relation to any Contract with the Purchaser the Supplier or any person employed by him or acting on his behalf has committed an offence under the Bribery Act 2010 or the Prevention of Corruption Acts 1889 to 1916 or having paid or offered any fee or reward contrary to Section 68 of the Local Government (Scotland) Act 1973; or

(k) the Supplier fails to conform to the terms and conditions of the Contract or fails to observe or perform any of its obligations under the Contract, and if such failure is capable of remedy the Supplier fails to remedy such failure within thirty (30) days of being required by the Purchaser in writing to do so; or

(l) Without prejudice to any other of the Purchaser's rights, in the event the Contract is terminated under this Condition 19.3, by whatever means, the Purchaser shall be entitled to enter into another Contract with a third party to carry out, deliver and complete the Services and the Supplier shall be liable for the Purchasers proper and reasonable losses, expenses, costs and charges in connection thereof. The Purchaser shall be entitled to recover said losses, expenses, costs and charges from the Supplier in accordance with Condition 20 (Recovery of Sums Due).

19.4 Notwithstanding any other rights under the Contract or otherwise in law, either Party shall be entitled to terminate this Contract by giving to the other Party not less than thirty (30) days' notice in writing to that effect. On the expiration of the said notice period the Contract shall in all respects cease and terminate.

19.5 The Supplier shall give notice to the Purchaser as soon as reasonably practicable if the Supplier is unable permanently or temporarily to meet any of the conditions of the Contract, or to observe or perform any of its obligations under the conditions of the Contract.

19.6 Termination under Conditions 19.2, 19.3, or 19.4, shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereupon accrue to the Purchaser and shall not affect the continued operation of Conditions 12 (Audit), 14 (Intellectual Property Rights), and 27 (Transfer of Undertakings (Protection of Employment)).

20. Recovery of Sums Due

20.1 Wherever under this Contract any sum of money is recoverable from or payable by the Supplier, that sum may be deducted from any sum then due, or which at any later time may become due, to the Supplier under this Contract or under any other agreement or contract with the Purchaser.

21. Assignation and Sub-Contracting

21.1 The Supplier shall not assign or sub-contract any portion of the Contract without the prior written consent of the Purchaser. Sub-contracting any part of the Contract shall not relieve the Supplier of any obligation or duty attributable to the Supplier under the Contract or these Conditions.

21.2 Where the Purchaser has consented to the placing of any Sub-Contract(s), the Purchaser reserves the right to obtain and keep copies of any Sub-Contract(s) from the Supplier, and the Supplier shall send copies of any Sub-Contract(s) to the Purchaser immediately at the Purchasers request.

21.3 Where the Purchaser has consented to the placing of any Sub-Contract, and the Supplier enters into a Sub-Contract, the Supplier must ensure that provisions are included which:

21.3.1 requires payment to be made of all sums due by the Supplier to the sub-contractor within a specified period not exceeding thirty (30) days from the receipt of a valid invoice as defined by the sub-contract requirements and provides that, where the Purchaser has made payment to the Supplier in respect of the Services, or any part of the Services, and the sub-contractor's invoice relates to such Services then, to that extent, the invoice must be treated as valid and, provided the Supplier is not exercising a right of retention or set-off in respect of a breach of contract by the sub-contractor or in respect of a sum otherwise due by the sub-contractor to the Supplier, payment must be made to the sub-contractor without deduction;

21.3.2 notifies the sub-contractor that the Sub-Contract forms part of a larger contract for the benefit of the Purchaser and that should the sub-contractor have any difficulty in securing the timely payment of an invoice, that matter may be referred by the sub-contractor, to the Purchaser;

21.3.3 provides the Supplier with a right to terminate the Sub-Contract if the relevant sub-contractor fails to comply in the performance of its Contract with any legal obligations in the fields of environmental, social or employment law, or if any of the termination events specified in Condition 19.3 occur;

21.3.4 requires the sub-contractor to include provisions having the same effect as Conditions 21.3.1, 21.3.2, and 21.3.3 above in any Sub-Contract it awards; and

21.3.5 in the same terms as that set out in this Condition 21.3 (including for the avoidance of doubt this Condition 21.3.5) subject only to modification to refer to the correct designation of the equivalent party as the Supplier, sub-contractor and sub-sub-contractor as the case may be.

21.3 Suppliers to the Purchaser are requested to address complaints regarding late payment of invoices to, in the first instance, the addressee of the invoice and, in the second instance to the Senior Manager (Corporate Procurement), 2nd Floor East, Cunninghame House, Irvine KA12 8EE or via email to procurement@north-ayrshire.gov.uk.

21.4 Any breach of this Condition 21 by the Supplier is a material breach for the purposes of Condition 19.2 (Termination).

22. Notices

22.1 Any notice to be given from one Party to the other under the Contract shall be valid only if it is made in writing.

22.2 Further any such notice which is to be given by either Party to the other, except for the purpose of court proceedings, shall be given by email or physical letter sent by hand or by a signed for special delivery postal service (for example, Royal Mail Signed For or Royal Mail Special Delivery Guaranteed). Such notices shall be addressed to the Supplier or to the Purchaser in the following manner –

22.2.1 For the Supplier – to the address shown on the Purchase Order, or to such other address as the Party may by notice to the other have substituted therefor in accordance with this Condition.

22.2.2 For the Purchaser – addressed to Senior Manager (Corporate Procurement), 2nd Floor East, Cunninghame House, Irvine KA12 8EE or via email to procurement@north-ayrshire.gov.uk, or to such other address as the Party may by notice to the other have substituted therefor in accordance with this Condition.

22.3 Where a notice is delivered by hand, it shall be deemed to have been delivered when it is left and signed for at the relevant Party's address set out in Condition 22.2.

22.4 Where a notice is delivered by a signed for special delivery postal service, provided that it is not returned as undelivered, it shall be deemed to have been given at the earlier of: two (2) Working Days after the day on which the letter was posted, or acknowledgement of receipt of such a letter by the Supplier or the Purchaser.

22.5 Where a notice is delivered by email it shall be deemed effective on the day of transmission, unless such transmission is not done on a day in which is not a Working Day or occurs after 1700 hours in which case it shall be deemed effective on the next Working Day.

22.6 The Supplier shall advise the Purchaser, as soon as practicable and in any event no later than seven (7) days after any change, of a change of address for service by sending a notice in accordance with this Condition.

22.7 The Purchaser may change its address for service by sending a notice in accordance with this Condition.

22.8 The Purchaser shall not be responsible for any failure to intimate or delay in intimation arising out of or in consequence of the Supplier's omitting to advise the Purchaser of a change of the Supplier's address under this Condition.

23. Compliance with the Law etc.

23.1 Throughout the duration of the Contract the Supplier shall be bound and obliged to comply with all applicable law, Good Industry Practice and the standards relevant to the Services (including regulatory bodies). During the period of the Contract the Supplier shall produce such evidence as the Purchaser may require to satisfy the Purchaser that the Supplier has complied with this Condition.

24. Dispute Resolution

24.1 In the event of any dispute arising out of or in connection with the Contract between the Parties either Party shall serve a notice on the other Party outlining the terms of the dispute. The Parties must attempt in good faith and in a spirit of mutual trust and co-operation to resolve the dispute as a matter of urgency and no later than twenty (20) Working Days of either Party notifying the other of the dispute.

24.2 In the event of any dispute of an emergency nature arising out of or in connection with the Contract between the Parties the Purchaser shall be entitled to demand that the Supplier attempts in good faith and in a spirit of mutual trust and co-operation to resolve the dispute within any timescale as the Purchaser considers reasonable in the circumstances and the Supplier must comply. The Purchaser shall be the sole judge of what disputes are of an emergency nature.

24.3 Any dispute or difference arising out of or in connection with the Contract, including any question regarding its existence, validity or termination which cannot be resolved in good faith, shall be determined by the appointment of a single arbitrator to be agreed between the Parties, and failing agreement within fourteen (14) days after either Party has given to the other a written request to concur in

the appointment of an arbitrator, by an arbitrator to be appointed by the Scottish Arbitration Centre on the written application of either Party. The seat of the arbitration shall be in Scotland. The language used in the arbitral proceedings shall be English.

24.4 Any arbitration under Condition 24.3 is subject to the Arbitration (Scotland) Act 2010.

24.5 Nothing in this Condition 24 shall:

24.5.1 prevent the Parties from complying with, observing and performing all their obligations in respect of the Contract regardless of the nature of any dispute between them arising out of or in connection with the Contract and notwithstanding the referral of any such matter or dispute for resolution under this Condition; nor

24.5.2 diminish the Parties to the Contract's responsibilities in respect of contract administration.

25. Headings

25.1 The headings to Conditions shall not affect their interpretation.

26. Governing Law

26.1 These Conditions shall be governed by and construed in accordance with Scottish law and the Supplier hereby irrevocably submits to the jurisdiction of the Scottish courts. The submission to such jurisdiction shall not (and shall not be construed so as to) limit the right of the Purchaser to take proceedings against the Supplier in any other court of competent jurisdiction, nor shall the taking of proceedings in any one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not.

27. Transfer of Undertakings (Protection of Employment)

27.1 The Supplier recognises that the Transfer of Undertakings (Protection of Employment) Regulations 2006 (**"TUPE"**) may apply in respect of the Contract, and that for the purposes of those Regulations, the undertaking concerned (or any relevant part of the undertaking) shall (a) transfer to the Supplier on the commencement of the Contract; (b) transfer to another Supplier on the expiry of the Contract.

27.2 During the period of six (6) months preceding the expiry of the Contract or after the Purchaser has given notice to terminate the Contract or the Supplier stops trading, and within twenty (20) Working Days of being so requested by the Purchaser, the Supplier shall fully and accurately disclose to the Purchaser or to any person nominated by the Purchaser information relating to employees engaged in providing the Services in relation to the Contract in particular, but not necessarily restricted to, the following:

(a) the total number of personnel whose employment with the Supplier is liable to be terminated at the expiry of this Contract but for any operation of law; and

(b) for each person, age and gender, details of their salary, date of commencement of continuous employment and pay settlements covering that person which relate to future dates, but which have already been agreed and their redundancy entitlements (the names of individual members of Staff do not have to be given); and

(c) information about the other terms and conditions on which the affected Staff are employed, or about where that information can be found; and

(d) details of pensions entitlements, if any.

27.3 The Supplier shall permit the Purchaser to use the information for the purposes of TUPE and of re-tendering, which shall include such disclosure to potential Suppliers as the Purchaser considers appropriate in connection with any re-tendering. The Supplier will co-operate with the re-tendering of the contract by allowing the transferee to communicate with and meet the affected employees and/or their representatives.

27.4 The Supplier agrees to indemnify the Purchaser fully and to hold it harmless at all times from and against all actions, proceedings, claims, expenses, awards, costs and all other liabilities whatsoever in any way connected with or arising from or relating to the provision or disclosure of information permitted under this Condition.

27.5 In the event that the information provided by the Supplier in accordance with this Condition becomes inaccurate, whether due to changes to the employment and personnel details of the affected employees made subsequent to the original provision of such information or by reason of the Supplier becoming aware that the information originally given was inaccurate, the Supplier shall notify the Purchaser of the inaccuracies and provide the amended information. The Supplier shall be liable for any increase in costs the Purchaser may incur as a result of the inaccurate or late production of data.

27.6 The provisions of this Condition 27 shall apply during the continuance of this Contract and after its termination howsoever arising.

28. Force Majeure

28.1 If either Party to this Contract is prevented or delayed in the performance of any of its obligations under this Contract as a direct result of a Force Majeure Event, and if such Party gives written notice to the other Party specifying the matters constituting the Force Majeure Event together with such evidence as it reasonably can give and specifying the period for which it is estimated that such prevention or delay will continue, then the Party in question shall be excused the performance or the practical performance as the case may be of such obligations in terms of this Contract which are so affected as from the date on which it became unable to perform them and for so long as the Force Majeure Event shall continue.

28.2 If the period during which either Party is delayed in or prevented from the performance of its obligations hereunder by reason of a Force Majeure Event

exceeds two (2) months, either Party may serve on the other one (1) months' notice of termination of the Contract.

28.3 Both Parties agree to use their best efforts to ensure that, during any period when a Force Majeure Event exists, the services are provided to the fullest extent practicable.

28.4 For the purposes of the Contract the expression "Force Majeure Event" shall mean any cause hindering the performance by a Party of its obligations, arising directly from acts, events or omissions beyond its reasonable control, including (but not limited to) fire, flood, or any disaster, epidemic, pandemic, war or civil unrest. Any act, event or omission will only be considered a Force Majeure Event if: (i) it's effects could not have been avoided or overcome by the affected Party, acting reasonably; and (ii) it is not attributable to the wilful act, neglect or failure to take reasonable precautions of the affected Party, its agents or employees.

29. Public Access to Information

29.1 No term of this Contract, whether express or implied, shall preclude the Purchaser from making public, if required under the Freedom of Information (Scotland) Act 2002 (referred to in this Condition as the "2002 Act") or the Environmental Information (Scotland) Regulations 2004 (referred to in this condition as "the EIRS") or both any information held relating to the Contract. In exercising its obligations under the 2002 Act and the EIRS, the Purchaser shall have due regard to the commercial interests of the Supplier but without prejudice to its duty to discharge its obligations under the 2002 Act or the EIRS. The interpretation of the Acts by the Purchaser, and any exemptions therein, will be final and conclusive subject only to any decision or binding ruling on the matter made by the courts. The Supplier will facilitate compliance by the Purchaser, with its obligations under the 2002 Act and the EIRS and comply with any requests from the Purchaser, for that purpose.

30. Change of Name / Contract Novation

30.1 If the Supplier's company name changes during the Contract but their company registration remains the same, the Supplier will be required to provide a copy of their "Certificate of Incorporation on Change of Name" at the earliest opportunity.

30.2 Where the company registration number changes the Supplier must inform the Purchaser immediately of any changes.

30.3 Where there is a change to any of the following the Purchaser reserves the right to terminate the Contract with immediate effect:

- Location of service
- Management structure
- Staff providing the service
- Operational policies and procedures

30.4 Subject to the above the Purchaser reserves the right to consider continuing the Contract with the new company provided that the company:

(a) meets any pre-qualification and minimum conditions that were applied when the original Contract was awarded.

(b) scores at least the same scores for the quality criteria that were applied at the procurement evaluation stage.

(c) signs a Deed of Novation confirming that they accept all contractual obligations and liabilities contained within the Contract.

31. Advertising

31.1 The Supplier shall not use the North Ayrshire Council logo without the prior written consent of the Purchaser.

31.2 The Supplier shall not disclose any details relating to Contract performance and operations with the Purchaser to any other party without the prior written consent of the Purchaser.

31.3 The Supplier shall not communicate in any form with the media, or make any publication or announcement, on any matter concerning the operation, involvement in or performance of the Contract, without the prior written consent of the Purchaser.

32. Data Protection

32.1 The Data Schedule will define the data relationship and dependent on this either paragraph 31.2 or 31.3 shall be applicable. Where there are aspects of duality within the relationship then both paragraphs 31.2 and 31.3 shall apply.

32.2 The Supplier acknowledges that Personal Data described in the scope of Schedule 1 (Data Protection) will be processed in connection with the Services under this Contract. For the purposes of any such Processing, Parties agree that the Supplier acts as the Data Processor and the Purchaser acts as the Data Controller.

32.3 Notwithstanding Condition 31.2, the parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Laws in respect of the Personal Data described in Schedule 1 as being under Joint Control. In respect of Personal Data under Joint Control, Conditions 31.1 to 31.16 (under exception of 31.3) will not apply and the Parties agree to put in place a Data Sharing and Processing Contract (Controller to Controller).

32.4 Both Parties agree to negotiate in good faith any such amendments to this Contract that may be required to ensure that both Parties meet all their obligations under Data Protection Laws. The provisions of this Condition 31 are without prejudice to any obligations and duties imposed directly on the Supplier under Data Protection Laws and the Supplier hereby agrees to comply with those obligations and duties.

32.5 The Supplier will, in conjunction with the Purchaser and in its own right and in respect of the Services, make all necessary preparations to ensure it will be compliant with Data Protection Laws.

32.6 The Supplier will provide the Purchaser with the contact details of its data protection officer or other designated individual with responsibility for data protection and privacy to act as the point of contact for the purpose of observing its obligations under the Data Protection Laws.

32.7 The Supplier must:

32.7.1 agree and comply with the terms of the data processing provisions set out in Schedule 1 (Data Protection);

32.7.2 process Personal Data only as necessary in accordance with obligations under the Contract and any written instructions given by the Purchaser (which may be specific or of a general nature), including with regard to transfers of Personal Data outside the United Kingdom unless required to do so by any legal or regulatory requirement to which the Supplier is subject; in which case the Supplier must inform the Purchaser of that legal or regulatory requirement (unless prohibited from doing so by law) before Processing the Personal Data only to the extent, and in such manner as is necessary for the performance of the Supplier's obligations under this Contract or as is required by the Law;

32.7.3 subject to Condition 31.7.2 only Process or otherwise transfer any Personal Data in or to any country outside the United Kingdom in accordance with the Data Protection Laws and with the Purchaser's prior written consent and subject to a security risk assessment being undertaken;

32.7.4 take all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that the Supplier Personnel:

(a) are aware of and comply with the Supplier's duties under this Condition;

(b) are subject to appropriate confidentiality undertakings with the Supplier or the relevant sub-contractor;

(c) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Purchaser or as otherwise permitted by this Contract; and

(d) have undergone adequate training in the use, care, protection and handling of Personal Data

32.7.5 implement appropriate technical and organisational measures including those set out in Schedule 1 (Data Protection) and in accordance with Article 32 of the UK GDPR to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, such measures being appropriate to the harm which might result from any unauthorised or unlawful Processing accidental loss, destruction or damage to the Personal

Data and having regard to the nature of the Personal Data which is to be protected and complete the security risk assessment.

32.8 The Supplier shall not engage a sub-contractor to carry out Processing in connection with the Services without prior specific or general written authorisation from the Purchaser. In the case of general written authorisation, the Supplier must inform the Purchaser of any intended changes concerning the addition or replacement of any other sub-contractor and give the Purchaser an opportunity to object to such changes.

32.9 If the Supplier engages a sub-contractor for carrying out Processing activities on behalf of the Purchaser, the Supplier must ensure that same data protection obligations as set out in this Contract are imposed on the sub-contractor by way of to implement appropriate technical and organisational measures. The Supplier shall remain fully liable to the Purchaser for the performance of the sub-contractor's performance of the obligations.

32.10 The Supplier must provide to the Purchaser reasonable assistance including by such technical and organisational measures as may be appropriate in complying with Articles 12-23 of the UK GDPR, including any subject access request and/or responding to any enquiry made, or investigation or assessment of processing initiated by the Information Commissioner in respect of the Personal Data as soon as is possible but in any event within three (3) business days of receipt of the request or any other period as agreed in writing with the Data Controller from time to time.

32.11 Taking into account the nature of the Processing and the information available, the Supplier must assist the Purchaser in complying with the Purchaser's obligations concerning the security of Processing, reporting requirements for Data Breaches, data protection impact assessments and prior consultations in accordance with Articles 32 to 36 of the UK GDPR. These obligations include:

(a) ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the Processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

(b) notifying a Data Breach to the Purchaser without undue delay and in any event no later than 24 hours after becoming aware of a Data Breach;

(c) assisting the Purchaser with communication of a Personal Data Breach to a Data Subject;

(d) supporting the Purchaser with preparation of a data protection impact assessment; and

(e) supporting the Purchaser with regard to prior consultation of the Supervisory Authority.

32.12 At the end of the provision of Services relating to Processing the Supplier must, on written instruction of the Purchaser, delete or return to the Purchaser all Personal Data and delete existing copies unless storage of the Personal Data is required by law.

32.13 The Supplier must:

(a) provide such information as is necessary to enable the Purchaser to satisfy itself of the Supplier's compliance with this Condition 31;

(b) allow the Purchaser, its employees, auditors, authorised agents or advisers reasonable access to any relevant premises, during normal business hours, to inspect the procedures, measures and records referred to in this Condition 31 and contribute as is reasonable to those audits and inspections;

(c) inform the Purchaser if in its opinion an instruction from the Purchaser infringes any obligation under the Data Protection Laws.

32.14 Parties acknowledge that the inspecting Party will use reasonable endeavours to carry out any audit or inspection under Condition 31.13 (b) with minimum disruption to the Supplier's day to day business.

32.15 The Supplier must maintain written records including in electronic form, of all Processing activities carried out in performance of the Services or otherwise on behalf of the Purchaser containing the information set out in Article 30(2) of the UK GDPR.

32.16 If requested, the Supplier must make such records referred to in Condition 31.15 available to the Supervisory Authority on request and co-operate with the Supervisory Authority in the performance of its tasks.

33. Security and Data

33.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Purchaser Data.

33.2 The Supplier shall not store, copy, disclose, or use the Purchaser Data except as necessary for the performance by the Supplier of its obligations under this Contract or as otherwise expressly authorised in writing by the Purchaser.

33.3 The Supplier shall preserve the integrity of the Purchaser Data and prevent the corruption or loss of the Purchaser Data, ensuring at all times that the relevant Purchaser Data is under its control or the control of any sub-contractor.

33.4 The Supplier shall perform secure back-ups of all Purchaser Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the BCDR Plan. The Supplier shall ensure that such back-ups are available to the Purchaser (or to such other person as the Purchaser may direct) at all times upon request and are delivered to the Purchaser at such other intervals as may be agreed in writing between the Parties.

33.5 The Supplier shall ensure that any system on which the Supplier holds any Purchaser Data, including back-up data, is a secure system that complies with the Security Plan. Where appropriate, the system should reflect the Scottish Public Sector Supply Chain Cyber Security Policy for cloud-based requirements as the same may be updated from time to time.

33.6 The Supplier shall at all times when performing the Services comply with the terms of the BCDR Plan.

33.7 If any of the Purchaser Data is corrupted, lost or sufficiently degraded as a result of the Suppliers default so as to be unusable, the Purchaser may:

33.7.1 require the Supplier (at the Supplier's expense) to restore or procure the restoration of Purchaser Data to the extent and in accordance with the requirements specified in **Error! Reference source not found.**3 (Business C ontinuity and Disaster Recovery) and the Supplier shall do so as soon as practicable but not later than five (5) Working Days from the date of receipt of the Purchaser's notice; and/or

33.7.2 itself restore or procure the restoration of Purchaser Data, and shall be repaid by the Supplier any reasonable expenses incurred in doing so to the extent and in accordance with the requirements specified in **Error! Reference s ource not found.** (Business Continuity and Disaster Recovery).

33.8 If at any time the Supplier suspects or has reason to believe that Purchaser Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Supplier shall notify the Purchaser immediately and inform the Purchaser of the remedial action the Supplier will take, subject to the Purchaser's prior written approval. The Purchaser reserves the right to demand the Supplier take any remedial action which the Purchaser considers necessary, acting reasonably, and the Purchaser shall do so as soon as practicable but not later than five (5) Working Days from the date of the Purchaser's notice

33.9 The Supplier shall comply with the requirements of Schedule 2 (Security Management).

34. Malicious Software

34.1 The Supplier shall, as an enduring obligation throughout the Contract, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor (unless otherwise agreed in writing between the Parties) to check for, actively monitor for, contain the spread of, and minimise the impact of, Malicious Software in relation to the Purchaser's System and the Supplier's System.

34.2 Notwithstanding clause 0, if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Purchaser Data, assist each other to restore the Services to their desired operating efficiency.

34.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of clause 0 shall be borne by the Parties as follows:

34.3.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Purchaser Data (whilst the Purchaser Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Purchaser when provided to the Supplier; and

34.3.2 otherwise by the Purchaser.

Schedule 1 (Data Protection)

Data Processing provision as required by Article 28(3) of the UK GDPR.

This Schedule includes certain details of the Processing of Personal Data in connection with the Services:

Subject matter and duration of the Processing of Personal Data

The subject matter and duration of the Processing of Personal Data are

---

The nature and purpose of the Processing of Personal Data

The type of Personal Data to be Processed

The categories of Data Subject to whom Personal Data related

The obligations and rights of the Purchaser

The obligations and rights of the Purchaser as the Data Controller are set out in Condition 31 of the Contract.

Schedule 2 (Security Management)

Guidance notes: Text in **red** requires to be amended/updated by the Purchaser to reflect the specific circumstances of this Contract.

1. Definitions

1.1 In this Schedule:

1.1.1 the following definitions shall apply:

"**Security Policy Framework**" means the Security Policy Framework published by the Cabinet Office as updated from time to time including any details notified by the Purchaser to the Supplier; and

"**Security Tests**" means both (a) tests carried out where relevant in accordance with the CHECK Scheme or to an equivalent standard to validate the Security Plan and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Arrangements

2.1 Both Parties shall provide a reasonable level of access to any members of their personnel for the purposes of designing, implementing and managing security in relation to the Services.

2.2 The Supplier shall ensure the up-to-date maintenance of a suitable security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Purchaser.

2.3 The Supplier shall comply with, implement and maintain all security measures :

(a) as may be required under applicable laws (including the Network and Information Systems Regulations 2018);

(b) to enable it to discharge its obligations under this Schedule 2; and

(c) to ensure there are no Breaches of Security;

in all cases to the Purchaser's reasonable satisfaction and in accordance with Good Industry Practice.

2.4 The Supplier shall notify the Purchaser promptly of any changes in its ability to meet the requirements of this Schedule 2, including any changes to certifications and accreditations.

2.5 The Supplier shall assist the Purchaser to comply with any applicable security requirements, codes, policies and practices in connection with the Services and/or this Contract.

Guidance notes: the Purchaser should consider whether paragraph 2.5 should be included in the Contract.

2.6 The Supplier warrants and undertakes that it shall meet and comply with this Schedule 2 in connection with the provision of the Services and this Contract (including in respect of any certification or accreditation).

2.7 The Supplier shall on demand indemnify the Purchaser and keep the Purchaser indemnified fully against all losses, liabilities, damages, costs and expenses (including legal and other professional fees) which may arise out of, or in consequence of, a breach of the warranty in paragraph 2.6 by the Supplier or the Supplier's Representatives.

3. Security Plan

3.1 Within twenty (20) Working Days after the commencement date, the Supplier shall prepare and submit to the Purchaser for approval in accordance with paragraph 3.3 a fully developed, complete and up-to-date Security Plan which shall comply with the requirements of paragraph 3.2.

3.2 The Security Plan shall:

3.2.1 meet the following requirements:

(a) [ISO/IEC 27001 and ISO/IEC 27002];

(b) Specification / Service Specification

(c) [set out here any other standard that the Supplier is required to meet]

[and, where not specifically addressed by (a) to (d) above, ensure that controls are in place to combat common threats as described in the [Cyber Essentials scheme (such as the "**5 technical controls**").]]

3.2.2 at all times provide a level of security which:

(a) is in accordance with Law and this Contract;

(b) as a minimum demonstrates Good Industry Practice;

(c) addresses issues of incompatibility with the Suppliers own organisational security policies;

(d) meets any specific security threats of immediate relevance to the Services and/or the Purchaser Data;

(e) complies with the security requirements as set out in the Service Specification;

(f) complies with the Purchaser's IT policies;

(g) is in accordance with the UK Government's Security Policy Framework; and

(h) meets the requirements and standards specified at paragraph 3.2.1 of this Schedule 2;

3.2.3 document the security incident management processes and incident response plans applicable to the Services;

3.2.4 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Purchaser approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy;

3.2.5 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

3.2.6 detail the process for managing any security risks from sub-contractors and third parties authorised by the Purchaser with access to the Services, processes associated with the delivery of the Services, the Purchaser Property, the Premises, the Supplier's System, the Purchaser's System (to the extent that it is under the control of the Supplier) and any IT, information and data (including the Purchaser Confidential Information and the Purchaser Data) and any system that could directly or indirectly have an impact on that information, data and/or the Services;

3.2.7 unless otherwise specified by the Purchaser in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Purchaser Property, the Premises , the Supplier's System, the Purchaser's System (to the extent that it is under the control of the Supplier) and any IT, information and data (including the Purchaser Confidential Information and the Purchaser Data) to the extent used by the Purchaser or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that information, data and/or the Services;

3.2.8 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with

and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule;

3.2.9 cross reference, if necessary, other Schedules which cover specific areas included within security standards and requirements which the Supplier is required to meet under this Contract;

3.2.10 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Purchaser engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule; and

3.2.11 be in accordance with the Security Policy Framework.

3.3 The Supplier shall update the Security Plan in accordance with any comments from the Purchaser, and shall review and revise the Security Plan regularly (or as per such other time period as agreed between the Parties) all in accordance with paragraph **Error! Reference source not found.** (such updates shall incorporate any comments received from the Purchaser).

3.4 The Supplier shall deliver all Services in accordance with the Security Plan.

4. Amendment and Revision of the Security Plan

4.1 The Security Plan shall be fully reviewed and updated by the Supplier regularly to reflect:

4.1.1 emerging changes in Good Industry Practice;

4.1.2 any change or proposed change to the IT Environment, the Services and/or associated processes;

4.1.3 any new perceived or changed security threats; and

4.1.4 any reasonable change in requirement requested by the Purchaser.

4.2 The Supplier shall provide the Purchaser 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 Purchaser. The results of the review shall include, without limitation:

4.2.1 suggested improvements to the effectiveness of the Security Plan;

4.2.2 updates to the risk assessments;

4.2.3 proposed modifications to respond to events that may impact on the Security Plan including the security incident management process, incident response plans and general procedures and controls that affect information security; and

4.2.4 suggested improvements in measuring the effectiveness of controls.

4.3 Subject to paragraph **Error! Reference source not found.**, any change w hich the Supplier proposes to make to the Security Plan (as a result of a review carried out pursuant to paragraph 4.1, a Purchaser request, a change to Service Specification, or otherwise) shall be subject to the Purchaser's prior written approval.

5. Security Testing

5.1 The Supplier shall conduct relevant Security Tests from time to time (not less frequently than annually). Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Purchaser. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Key Performance Indicators, if applicable, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

5.2 The Supplier shall provide the Purchaser with the results of such tests (in a form approved by the Purchaser in advance) as soon as practicable after completion of each Security Test.

5.3 Where any Security Test carried out reveals any actual or potential Breaches of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Purchaser of any changes to the Security Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Purchaser's prior written approval, the Supplier shall implement such changes to the Security Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Purchaser or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan is to address a non-compliance with the security requirements (as set out in the Service Specification) and/or elsewhere in the Contract) or the requirements of this Schedule, the change to the Security Plan shall be at no cost to the Purchaser.

5.4 If any repeat Security Test carried out pursuant to paragraph 5.3 reveals actual or potential Breaches of Security exploiting the same root cause failure, such circumstance shall be deemed to constitute a material breach that is capable of remedy.

6. Security Plan Compliance, Information and Audit

6.1 Promptly upon request, the Supplier shall provide to the Purchaser such information and records in connection with the Supplier's obligations under this Schedule 2 as the Purchaser may request.

6.2 The Purchaser shall be entitled to carry out such security audits as it may reasonably deem necessary in order to:

6.2.1 ensure that the Security Plan maintains compliance with the requirements and standards set out at paragraph 3.2 (Security Plan) of this Schedule 2 and the Baseline Security Requirements;

6.2.2 ascertain the impact of any Breaches of Security;

6.2.3 review and verify the integrity, confidentiality and security of any data relating to this Contract; and/or

6.2.4 review the Supplier's and/or any sub-contractor's compliance with its obligations under this Schedule 2.

6.3 The Supplier shall (and shall ensure that any sub-contractor shall) provide the Purchaser, its agents and representatives with all reasonable co-operation and assistance in relation to audits, including but not limited to:

6.3.1 all data and/or records requested by the Purchaser;

6.3.2 access to any relevant premises and to any equipment owned/controlled by the Supplier, any associated or group company and any sub-contractor and, where such premises and/or equipment are out with the control of the Supplier, shall secure sufficient rights of access for the Purchaser, its agents and representatives as are necessary to allow audits to take place; and

6.3.3 access to any relevant individuals.

Guidance notes: The Supplier may not be able to facilitate an audit of its sub-contractors in all cases (for example, this may not be possible if the Supplier is using some major public cloud providers). In such circumstances, the Purchaser should carefully consider its requirements with regard to assurance.

6.4 If, on the basis of evidence provided by such audits, it is the Purchaser's reasonable opinion that compliance with the security requirements of this Schedule 2 and the rest of the Contract and/or the Baseline Security Requirements is not being achieved by the Supplier, then the Purchaser shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement any necessary remedy. If the Supplier does not become compliant within the required time, then the Purchaser shall have the right to obtain an independent audit against these requirements and standards in whole or in part.

6.5 If, as a result of any such independent audit as described in paragraph 6.2 the Supplier is found to be non-compliant with the security requirements of this Schedule 2 and/or the rest of the Contract and/or the Baseline Security Requirements, then the Supplier shall, at its own expense, immediately undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Purchaser in obtaining such audit.

7. Breach of Security

7.1 Each Party shall promptly notify the other in accordance with the agreed security incident management process as defined by the Security Plan upon becoming aware that any Breaches of Security or attempted or potential Breaches of Security has or may have taken place.

7.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 7, the Supplier shall:

7.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Purchaser) necessary to:

(a) minimise the extent of actual or potential harm caused by any Breaches of Security;

(b) remedy such Breaches of Security to the extent possible and protect the integrity of the Purchaser's System and the Supplier's System to the extent within its control against any such Breaches of Security or attempted or potential Breaches of Security and provide the Purchaser details of any mitigation measures recommended by the Supplier to be taken by the Purchaser in respect of the Purchaser's System within the control of the Purchaser;

(c) apply a tested mitigation against any such Breaches of Security or attempted or potential Breaches of Security and, provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to deliver the Services so as to meet the Key Performance Indicators(if applicable), the Supplier shall be granted relief against any resultant under-performance for such period as the Purchaser, acting reasonably, may specify by written notice to the Supplier;

(d) prevent any further Breaches of Security or attempted or potential Breaches of Security in the future exploiting the same root cause failure; and

(e) supply any requested data to the Purchaser within two (2) Working Days of the Purchaser's request and without charge (where such requests are reasonably related to a possible incident or compromise); and

7.2.2 investigate the Breaches of Security or attempted or potential Breaches of Security completely and promptly and as soon as reasonably practicable provide to the Purchaser full details (using the reporting mechanism defined by the Security Plan) of the Breaches of Security or attempted or potential Breaches of Security, including a root cause analysis where required by the Purchaser.

7.3 If any action is taken in response to any Breaches of Security or potential or attempted Breaches of Security that demonstrates non-compliance of the

Security Plan with the Baseline Security Standards or the requirements of this Schedule, then any required change to the Security Plan shall be at no cost to the Purchaser.

7.4 Following any of the circumstances referred to in paragraph 7, the Supplier shall:

(a) where required to do so, inform any applicable regulator of the Breaches of Security or attempted or potential Breaches of Security; and

(b) take any action deemed necessary by the Purchaser in the circumstances, including complying with any additional security measures deemed appropriate by the Purchaser.

8. Vulnerabilities and Corrective Action

8.1 The Purchaser and the Supplier acknowledge that from time to time vulnerabilities in the Purchaser's System, the Supplier's System and the Services will be discovered which unless mitigated will present an unacceptable risk to the Purchaser's information, including Purchaser Data.

8.2 The severity of threat vulnerabilities for the Services shall be categorised by using an appropriate vulnerability scoring systems including:

8.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST; and/or

8.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

8.3 The Supplier shall ensure the application of security patches to vulnerabilities in a timely and prioritised manner.

8.4 The Supplier shall ensure all COTS Software is upgraded within six (6) months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Contract.

8.5 The Supplier shall:

8.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Government Body;

8.5.2 ensure that the Purchaser's System and the Supplier's System (to the extent within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

8.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Purchaser's System, the Supplier's System and the Services by actively monitoring the threat landscape during the Contract;

8.5.4 pro-actively scan the Purchaser's System and the Supplier's System (to the extent within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the Security Plan as developed under paragraph 3.2.1;

8.5.5 from the date specified in the Security Plan, provide a report to the Purchaser within five (5) Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the Purchaser's System and the Supplier's System (to the extent within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

8.5.6 propose interim mitigation measures to vulnerabilities in the Purchaser's System, and the Supplier's System known to be exploitable where a security patch is not immediately available;

8.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Purchaser's System and the Supplier's System); and

8.5.8 inform the Purchaser when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Services, the Purchaser's System and the Supplier's System and provide initial indications of possible mitigations.

8.6 If the Supplier is unlikely to be able to mitigate the vulnerability within a timely manner under paragraph **Error! Reference source not found.**, the Supplier shall immediately notify the Purchaser.

9. Breach of Security Requirements

9.1 A breach of this Schedule 2 by the Supplier is a material breach for the purposes of Condition 19.2.

9.2 If the Supplier fails to comply with the provisions of this Schedule 2, the Purchaser may take any action it considers appropriate or necessary (and the Supplier shall comply with the Purchaser's requests in this respect), including:

(a) suspending the whole or any part of the Supplier's obligations under this Contract;

(b) requiring that any Supplier Representative connected with such breach be removed from their involvement with the Services and this Contract and cease to have any access to the Purchaser's Protected Information

and any Personal Data in connection with the Services under this Contract;

(c) requesting the Supplier return and/or arrange the evidenced secure and permanent destruction of the Purchaser's Protected Information and any Personal Data in connection with the Services under this Contract; and

(d) implementing additional or alternative measures, both technical and organisational, to protect and secure the Purchaser's Protected Information and any Personal Data in connection with the Services under this Contract.

Schedule 3 (Business Continuity and Disaster Recovery(BDCR))

1. BCDR Plan

1.1 Within sixty (60) Working Days from the commencement date the Supplier shall prepare and deliver to the Purchaser for the Purchaser's written approval a plan, which shall detail the processes and arrangements that the Supplier shall follow to:

1.1.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services; and

1.1.2 the recovery of the Services in the event of a Disaster.

1.2 The BCDR Plan shall:

1.2.1 be divided into three parts:

(a) Part A which shall set out general principles applicable to the BCDR Plan;

(b) Part B which shall relate to business continuity (the "**Business Continuity Plan**"); and

(c) Part C which shall relate to disaster recovery (the "**Disaster Recovery Plan**"); and

1.2.2 unless otherwise required by the Purchaser in writing, be based upon and be consistent with the provisions of paragraphs 2, 3 and 4.

1.3 Following receipt of the draft BCDR Plan from the Supplier, the Purchaser shall:

1.3.1 review and comment on the draft BCDR Plan as soon as reasonably practicable; and

1.3.2 notify the Supplier in writing that it approves or rejects the draft BCDR Plan no later than twenty (20) Working Days after the date on which the draft BCDR Plan is first delivered to the Purchaser.

1.4 If the Purchaser rejects the draft BCDR Plan:

1.4.1 the Purchaser shall inform the Supplier in writing of its reasons for its rejection; and

1.4.2 the Supplier shall then revise the draft BCDR Plan (taking reasonable account of the Purchaser's comments) and shall re-submit a revised draft BCDR Plan to the Purchaser for the Purchaser's approval within twenty (20) Working Days of the date of the Purchaser's notice of rejection. The provisions of paragraph 1.3 and this paragraph 1.4 shall apply again to any resubmitted draft BCDR Plan, provided that either

Party may refer any disputed matters for resolution in accordance with the procedure outlined in Condition 24 (Dispute Resolution).

2. Part A of the BCDR Plan and General Principles and Requirements

2.1 Part A of the BCDR Plan shall:

2.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

2.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the operation of the Services and any services provided to the Purchaser by a Related Supplier;

2.1.3 contain an obligation upon the Supplier to liaise with the Purchaser and (at the Purchaser's request) any Related Supplier with respect to issues concerning business continuity and disaster recovery where applicable;

2.1.4 detail how the BCDR Plan links and interoperates with any overarching and/or connected disaster recovery or business continuity plan of the Purchaser and any of its other Related Suppliers in each case as notified to the Supplier by the Purchaser from time to time;

2.1.5 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 Purchaser;

2.1.6 contain a risk analysis, including:

(a) failure or disruption scenarios and assessments and estimates of frequency of occurrence;

(b) identification of any single points of failure within the Services and processes for managing the risks arising therefrom;

(c) identification of risks arising from the interaction of the Services with the services provided by a Related Supplier; and

(d) a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;

2.1.7 provide for documentation of processes, including business processes, and procedures;

2.1.8 set out key contact details (including roles and responsibilities) for the Supplier (and any sub-contractors) and for the Purchaser;

2.1.9 identify the procedures for reverting to “**normal service**”;

2.1.10 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 more than the accepted amount of data loss and to preserve data integrity;

2.1.11 identify the responsibilities (if any) that the Purchaser has agreed in writing that it will assume in the event of the invocation of the BCDR Plan; and

2.1.12 provide for the provision of technical advice and assistance to key contacts at the Purchaser as notified by the Purchaser from time to time to inform decisions in support of the Purchaser's business continuity plans.

2.2 The BCDR Plan shall be designed so as to ensure that:

2.2.1 the Services are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

2.2.2 the adverse impact of any Disaster, service failure, or disruption on the operations of the Purchaser is minimal as far as reasonably possible;

2.2.3 it complies with the relevant provisions of ISO/IEC 27002, ISO/IEC 22301 and all other industry standards from time to time in force; and

2.2.4 there is a process for the management of disaster recovery testing detailed in the BCDR Plan.

2.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Services or to the business processes facilitated by and the business operations supported by the Services.

2.4 The Supplier shall not be entitled to any relief from its obligations under the Key Performance Indicators(if applicable) or to any increase in the prices to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

3. Business Continuity Plan – Principles and Contents

3.1 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 Services remain supported and to ensure continuity of the business operations supported by the Services including, unless the Purchaser expressly states otherwise in writing:

3.1.1 the alternative processes (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to the Services; and

3.1.2 the steps to be taken by the Supplier upon resumption of the Services in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

3.2 The Business Continuity Plan shall:

3.2.1 address the various possible levels of failures of or disruptions to the Services;

3.2.2 set out the services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services (such services and steps, the "**Business Continuity Services**");

3.2.3 specify any applicable Key Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Key Performance Indicators , if applicable, in respect of other Services during any period of invocation of the Business Continuity Plan; and

3.2.4 clearly set out the conditions and/or circumstances under which the Business Continuity Plan is invoked.

4. Disaster Recovery Plan – Principles and Contents

4.1 The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Purchaser supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

4.2 The Disaster Recovery Plan shall be invoked only upon the occurrence of a Disaster.

4.3 The Disaster Recovery Plan shall include the following:

4.3.1 the technical design and build specification of the Disaster Recovery System;

4.3.2 details of the procedures and processes to be put in place by the Supplier 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:

(a) backup methodology and details of the Supplier's approach to data back-up and data verification;

(b) identification of all potential disaster scenarios;

(c) risk analysis;

(d) documentation of processes and procedures;

(e) hardware/software configuration details;

(f) network planning including details of all relevant data networks and communication links;

(g) invocation rules;

(h) Services recovery procedures; and

(i) steps to be taken upon resumption of the Services to address any prevailing effect of the failure or disruption of the Services;

4.3.3 any applicable Key Performance Indicators with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the applicable Key Performance Indicators in respect of other Services during any period of invocation of the Disaster Recovery Plan;

4.3.4 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

4.3.5 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

4.3.6 testing and management arrangements.

5. Review and Amendment of the BCDR Plan

5.1 The Supplier shall review the BCDR Plan (and the risk analysis on which it is based):

5.1.1 on a regular basis and as a minimum once every six (6) months or as part of a major reconfiguration of the Services or the Supplier's supply chain;

5.1.2 within three (3) calendar months of the BCDR Plan (or any part) having been invoked pursuant to paragraph 7; and

5.1.3 where the Purchaser requests any additional reviews (over and above those provided for in paragraphs 5.1.1 and 5.1.2) by notifying the Supplier to such effect in writing, whereupon the Supplier shall conduct such reviews in accordance with the Purchaser's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Purchaser for the Purchaser's approval. The costs of both Parties of any such additional reviews shall be met by the Purchaser except that the Supplier shall not be entitled to charge the Purchaser for any costs that it may incur above any estimate without the Purchaser's prior written approval.

5.2 Each review of the BCDR Plan pursuant to paragraph 5.1 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 Services or any underlying business processes and operations facilitated by or supported by the 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 Supplier within the period required by the BCDR Plan or, if no such period is required, within such period as the Purchaser shall reasonably require. The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Purchaser a report (a "**Review Report**") setting out:

5.2.1 the findings of the review;

(a) any changes in the risk profile associated with the Services; and

(b) the Supplier's proposals (the "**Supplier'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 Supplier 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.

5.3 Following receipt of the Review Report and the Supplier's Proposals, the Purchaser shall:

5.3.1 review and comment on the Review Report and the Supplier's Proposals as soon as reasonably practicable; and

5.3.2 notify the Supplier in writing that it approves or rejects the Review Report and the Supplier's Proposals no later than twenty (20) Working Days after the date on which they are first delivered to the Purchaser.

5.4 If the Purchaser rejects the Review Report and/or the Supplier's Proposals:

5.4.1 the Purchaser shall inform the Supplier in writing of its reasons for its rejection; and

5.4.2 the Supplier shall then revise the Review Report and/or the Supplier's Proposals as the case may be (taking reasonable account of the Purchaser's comments and carrying out any necessary actions in connection with the revision) and shall re-submit a revised Review Report and/or revised Supplier's Proposals to the Purchaser for the Purchaser's approval within twenty (20) Working Days of the date of the Purchaser's notice of rejection. The provisions of paragraph 5.3 and this paragraph 5.4 shall apply again to any resubmitted Review Report and Supplier's Proposals, provided that either Party may refer any disputed matters for resolution in accordance with the procedure outlined in Condition24 (Dispute Resolution).

5.5 The Supplier shall as soon as is reasonably practicable after receiving the Purchaser's approval of the Supplier'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 Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can

be reasonably shown that the changes are required because of a material change to the risk profile of the Services.

6. Testing on the BCDR Plan

6.1 The Supplier shall test the BCDR Plan on a regular basis (and in any event not less than once every year). Subject to paragraph 6.2, the Purchaser may require the Supplier to conduct additional tests of some or all aspects of the BCDR Plan at any time where the Purchaser considers it necessary, including where there has been any change to the 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.

6.2 If the Purchaser requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Purchaser's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Purchaser unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

6.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with the Purchaser and shall liaise with the Purchaser in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Purchaser in this regard. Each test shall be carried out under the supervision of the Purchaser or its nominee.

6.4 The Supplier shall ensure that any use by it or any sub-contractor of "**live**" data in such testing is first approved with the Purchaser. Copies of live test data used in any such testing shall be (if so, required by the Purchaser) destroyed or returned to the Purchaser on completion of the test.

6.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Purchaser a report setting out:

6.5.1 the outcome of the test;

6.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

6.5.3 the Supplier's proposals for remedying any such failures.

6.6 Following each test, the Supplier shall take all measures requested by the Purchaser, (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 Supplier, at no additional cost to the Purchaser, by the date reasonably required by the Purchaser and set out in such notice.

6.7 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 Supplier of any of its obligations under this Contract.

6.8 The Supplier shall also perform a test of the BCDR Plan in the event of any major reconfiguration of the Services or as otherwise reasonably requested by the Purchaser.

7. Invocation of the BCDR Plan

In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Purchaser promptly of such invocation along with the anticipated maximum period of outage). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior written consent of the Purchaser.