SCHEDULE OF TERMS AND CONDITIONS

1 Provision of Goods and Services

1.1 The Supplier shall supply the Goods and Services for the Term and in accordance with the terms of this Agreement.

1.2 For the avoidance of doubt, no other terms and conditions shall apply to this Agreement. In particular, the Supplier's standard terms and conditions shall not apply to the provision of the Goods and Services notwithstanding any reference to such terms in any document. The Supplier waives any right which it otherwise might have to rely on its own terms and conditions.

1.3 Any performance or continued performance under the Agreement shall be deemed to constitute the Supplier's acceptance of the terms of this Agreement

2 Payment

2.1 Subject to Clause 2.6, in consideration of the Supplier providing the Goods and Services, John Lewis shall pay all valid invoices for Charges within 60 days of the later of the date of the invoice or the date on which John Lewis received the invoice.

2.2 The Supplier shall invoice John Lewis for the Charges in arrears following completion of the Services or delivery of the Goods. The Supplier shall ensure that all Charges for all Goods and Services provided are invoiced within one month of provision of the Goods and Services, as well as the provisions of this Clause 2.

2.3 All prices, rates and Charges referred to in this Agreement are exclusive of value added tax ("VAT") but inclusive of packaging, insurance, carriage and all other charges, taxes and duties. The Supplier shall identify any part of any invoice that is zero-rated or exempt from VAT with a full explanation.

2.4 John Lewis shall have the right to set off any payment due or which at any time may become due under a valid invoice against any sums owed to John Lewis by the Supplier under this Agreement or otherwise.

2.5 If any sum due and payable under this Agreement is not paid by John Lewis in accordance with the agreed payment terms then the Supplier shall provide written notice to John Lewis of such non-payment. The Supplier shall be entitled (without prejudice to any of its other rights) to charge interest at the rate of two per cent above the base rate of the Bank of England from time to time in force from the date such written notice is received by John Lewis until the date of actual payment. Interest shall not accrue or be payable where monies are set off or withheld pursuant to Clause 2.4. The parties agree that the right to claim interest under this Clause 2.5 is a substantial remedy for late payment and is in substitution for any statutory or other right to claim interest and/or other remedy for late payment under the Late Payment of Commercial Debts (Interest) Act 1998.

2.6 Notwithstanding Clause 2.1 above, John Lewis rationalises its payment cycle by processing supplier payments once a week. This means that invoice payments will be processed in the scheduled payment run on or following the invoice due date. The Supplier agrees that the Charges may therefore be paid by John Lewis up to six (6) days after the invoice due date specified in Clause 2.1. Payment under Clause 2.1 shall be deemed to have been made by John Lewis on the date that the money leaves John Lewis' bank account.

3 Confidentiality

3.1 Each party (a "**Receiving Party**") shall not at any time disclose to any person any and all confidential information disclosed to it by the other party (the "**Disclosing Party**") concerning the business or affairs of the Disclosing Party or of any member of the Disclosing Party's Group (for the purpose of this Agreement, "**Group**" shall mean a party, any subsidiary or holding company from time to time of that party, and any subsidiary from time to time of that party's holding companies, as such terms are defined in the Companies Act 2006 (or any replacement statutes)), including but not limited to information relating to the Disclosing Party's operations, pricing, processes, initiatives, plans, product information, technical or commercial know-how, specifications, inventions, designs, trade secrets, software, market opportunities and customers ("**Confidential Information**"), except as permitted by Clause 3.2.

3.2 The Receiving Party may disclose the Disclosing Party's Confidential Information:

(a) to the Receiving Party's, and to its Group's, employees, workers, officers, consultants, or professional advisers ("**Representatives**") who need to know such information for the purposes of carrying out the Receiving Party's obligations under this Agreement, provided that the Receiving Party shall ensure that its Representatives comply with the confidentiality obligations contained in this Clause 3 as though they were a party to this Agreement. The Receiving Party shall remain principally liable to the Disclosing Party where any Representative fails to comply with the obligations of confidence and security owed to the Disclosing Party under this Agreement;

(b) as may be required by law, court order or by any governmental or regulatory authority or any securities exchange to which the Receiving Party is subject; and

(c) to the extent the Confidential Information has become publicly available or generally known to the public at the time of the disclosure other than as a result of a breach of this Clause 3.

3.3 On completion, termination or other expiry of the Agreement, the Confidential Information and any records or copies of the same in whatever form, must be destroyed or returned promptly to the Disclosing Party at their request.

4 **Intellectual Property Rights**

4.1 Unless agreed between the parties, this Agreement does not assign or otherwise transfer any Intellectual Property Rights (for purposes of this Agreement, "**Intellectual Property Rights**" shall mean all intellectual property rights whether or not registered or registrable and including all extensions, renewals and applications thereof and including, without limitation, all patents, rights to inventions, copyright and related rights, trade marks, trade names, business names and domain names, design rights, goodwill, database rights, Confidential Information, trade secrets and know-how) existing at or prior to the Effective Date (the "**Pre-Existing IPR**"). Neither party may assert ownership of the other party's Pre-Existing IPR.

4.2 The Intellectual Property Rights that:

(a) arise, or are created or developed by either party; or

(b) are adapted from Pre-Existing IPR for John Lewis,

in connection with this Agreement and all items created through the performance of the Parties' obligations under this Agreement (together, the "**Foreground IPR**") shall, on creation of such rights and/or items, vest in John Lewis. The Supplier hereby assigns to John Lewis to the fullest extent possible and for John Lewis to hold absolutely, with full title guarantee and free from all third party rights and encumbrances, all such Foreground IPR.

4.3 John Lewis hereby grants to the Supplier a non-exclusive, royalty free licence to use its Pre-Existing IPR for the duration of this Agreement to the extent required to provide the Goods and/or Services and otherwise comply with its obligations under this Agreement. The Supplier may not assign, licence, grant security over or otherwise transfer John Lewis' Pre-Existing IPR.

4.4 The Supplier hereby grants to John Lewis a non-exclusive, royalty free licence to use its Pre-Existing IPR, in perpetuity to enable John Lewis to receive, use and enjoy the Goods and Services. John Lewis may at any time grant a licence to any member of its Group to use the Supplier's Pre-Existing IPR. Subject to the foregoing, John Lewis may not otherwise assign, licence, grant security over or otherwise transfer the other party's Pre-Existing IPR.

4.5 John Lewis grants to the Supplier a non-exclusive, royalty-free, non-transferable, non- sublicensable licence to use the Foreground IPR for the duration of this Agreement to the extent required to provide the Goods and/or Services and otherwise comply with its obligations under this Agreement.

4.6 The Supplier shall ensure and undertakes to procure that all moral rights, to which any individual is now or may be at any future time entitled under Chapter IV of Part I of the Copyright Designs and Patents Act 1988 or any similar provisions of law in any jurisdiction, in the Goods and any deliverables arising from the Services are waived irrevocably and unconditionally and are not asserted.

4.7 Neither party shall use any trade name, logo or other trade mark of the other party without the other party's prior written agreement.

4.8 The Supplier shall, promptly at John Lewis' request, do (or procure to be done) all such further acts and things and the execution of all such other documents as John Lewis may from time to time require for the purpose of securing for John Lewis the full benefit of the Agreement, including all right, title and interest in and to the Foreground IPR.

5 Data Protection

5.1 For the purposes of this clause 5:

(a) "**Data Protection Legislation**" shall mean, for the periods in which they are in force, the Data Protection Act 2018,, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003), the GDPR (as defined below) and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner, in each case as amended or substituted from time to time;

(b) **Data Subject** shall have the same meaning as in the GDPR;

(c) **GDPR** shall mean:

(i) the General Data Protection Regulations (Regulation (EU) 2016/679) which came into force on 25 May 2018; or

(ii) any equivalent legislation amending or replacing the General Data Protection Regulations (Regulation (EU) 2016/679);

(d) **Personal Data** shall have the meaning given to this term in the GDPR; and

(e) **Personal Data Breach** shall have the meaning given to this term in the GDPR.

5.2 The Supplier shall and shall procure that the Supplier Group and its Sub-contractors shall comply with all Data Protection Legislation in relation to any Personal Data processed (as that term is understood under the GDPR) relating to or originating from John Lewis, its employees or customers.

5.3 Upon request by John Lewis, the Supplier shall promptly provide to John Lewis such copies of any Personal Data provided by or on behalf of John Lewis to the Supplier under the Agreement and do such other acts in relation to the Personal Data or any part thereof as John Lewis shall request.

5.4 Without limiting Clause 5.2, the Supplier represents, warrants and undertakes to John Lewis that the Supplier:

(a) shall not by any act or omission put John Lewis in breach of the Data Protection Legislation;

(b) shall at all times comply with, and ensure that at all times its staff and sub-contractors comply with any instructions, guidelines, codes of practice, policies, instructions or other requirements (including without limitation any assistance in connection with the implementation of a Data Protection Impact Assessment) notified to it by John Lewis in connection with processing Personal Data (as defined by the GDPR, or any amendment to or replacement of the same);

(c) shall not transfer any Personal Data to any other person (including, without limitation, any data processor or other contractor) without John Lewis's prior written consent and unless permitted under Data Protection Legislation and, where consent is given by John Lewis, the Supplier shall only undertake such transfer in accordance with John Lewis's instructions;

(d) shall keep all Personal Data confidential and implement appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction or damage and it shall only deal with the Personal Data for the purposes, and in accordance with its obligations, set out in the Agreement so that the processing of Personal Data carried out by the Supplier meets the requirements of the Data Protection Legislation and ensures the protection of the rights of the Data Subjects;

(e) shall take all reasonable steps to ensure the reliability of any of its staff who have access to Personal Data processed in connection with the Agreement and ensure that its Staff shall be subject to obligations to maintain the confidentiality of Personal Data;

(f) shall take all reasonable steps to delete or fully and irreversibly anonymise Personal Data upon instruction by John Lewis and shall ensure that its sub-processors undertake such acts as required;

(g) shall keep detailed records of the processing of Personal Data and shall provide copies of all records to John Lewis on request;

(h) shall provide such information and, on reasonable prior notice, allow for and contribute to audits, including inspections, conducted by John Lewis or an auditor mandated by John Lewis as is reasonably necessary to enable John Lewis to satisfy itself of the Supplier's compliance with the Agreement and the Data Protection Legislation;

(i) shall not contact John Lewis Data Subjects directly or collect any Personal Data in relation to John Lewis Data Subjects without John Lewis' prior written consent;

(j) shall not use any sub-contractors to process Personal Data, unless John Lewis has issued its prior written consent and the Supplier shall ensure that sub-contracts entered into with approved sub-contractors shall include provisions equivalent to those in this Clause 5; and

(k) shall on termination of the Agreement, and at any time on John Lewis' request, immediately either return the Personal Data in the format requested by John Lewis or destroy the Personal Data (including all copies of it) and confirm in writing that it has complied with this obligation.

5.5 The Supplier shall not process Personal Data outside of the United Kingdom and/or the European Economic Area (as it is made up from time to time) (an "**International Transfer**") without John Lewis's prior written consent. If John Lewis gives its prior written consent, before making that International Transfer, the Supplier will demonstrate or implement, to John Lewis's satisfaction, appropriate safeguards for that International Transfer in accordance with the Data Protection Legislation and will ensure that enforceable rights and effective legal remedies for Data Subjects are available. Such appropriate safeguards may include:

(a) there is in force a European Commission decision that the country or territory to which the International Transfer is to be made ensures an adequate level of protection for Processing of Personal Data;

(b) the relevant data processor enters into an agreement with John Lewis; or

(c) the International Transfer is to the United States of America and the relevant processor has and maintains for the duration of the processing a current registration under the US-EU Privacy Shield.

5.6 If the appropriate safeguards demonstrated or implemented by the Supplier in accordance with this Clause are deemed at any time not to provide an adequate level of protection in relation to the Personal Data, the Supplier will implement such alternative measures as may be required by John Lewis to ensure that the relevant International Transfer and all resulting processing are compliant with the Data Protection Legislation.

5.7 On termination of the Agreement, and at any time on the request of John Lewis, at the option of John Lewis, either return the Personal Data to John Lewis or provide it to a replacement supplier in the format requested by John Lewis or destroy the Personal Data (including all copies of it), in each

case immediately and confirm in writing that it has complied with this obligation.

5.8 The Supplier shall notify John Lewis promptly and in any event within five (5) Business Days if it receives:

(a) any request submitted by or on behalf of a Data Subject with regard to that person's Personal Data (including a request from a Data Subject to exercise their rights under the Data Protection Legislation), including by appropriate technical and organisational measures insofar as this is possible; or

(b) a complaint or request relating to John Lewis's obligations and/or the rights of a Data Subject under the Data Protection Legislation; and

(c) any other communication relating directly or indirectly to the processing of any Personal Data.

5.9 In each case under Clause 5.8, irrespective of whether the Supplier or John Lewis received the initial request, complaint or communication directly, the Supplier shall promptly provide John Lewis with its full co-operation and assistance as is reasonably required by John Lewis in order to respond to and resolve the request, complaint or other communication within any time frames imposed by applicable Data Protection Legislation or any regulatory authority, and shall not respond to any such request or communication without the prior written consent of John Lewis.

5.10 The Supplier shall:

(a) notify John Lewis immediately using the email breach.notification@johnlewis.co.uk on becoming aware of any Personal Data Breach; and

(b) promptly following notification and in a timely manner so as to allow John Lewis to comply with its 72 hours Data Protection Legislation notification obligation, provide such information and assistance as is reasonably required by John Lewis in order for John Lewis to notify the Personal Data Breach or any other communication to the relevant Regulators and/or any Data Subjects.

5.11 If relevant to the Services, the Supplier shall at its own cost ensure that, throughout the Term, it shall be PCI compliant/PCI certified and the Services comply with Payment Card Industry Data Security Standards (PCIDSS) for the time being and the Supplier undertakes that its performance of the Agreement in accordance with its terms shall not be in breach of the PCIDSS. Furthermore, the Supplier acknowledges and agrees that it shall be responsible for the security of all cardholder data provided to it.

5.12 If relevant to the Services, the Supplier shall at its own cost ensure that, throughout the Term, any cookies, tags or similar technologies (the "**Cookies**") it provides the Partnership with, or directly places in any of the Partnership's websites, are previously approved by the Partnership.

5.13 This approval request shall be sent with the following information:

(a) Cookies' names

(b) Category of the Cookies:

(i) Persistent or session, and

(ii) Essential Cookies - cookies that are necessary to provide users with services that are provided by the website

(iii) Analytics and Performance Cookies - cookies that are used to collect information about how visitors use a website, in order to understand how to improve the site and its services;

(iv) Functionality Cookies - cookies that are used to enhance the functionality of the website, but are not essential to using the site; or

(v) Advertising Cookies - Used to make advertising message more relevant to the user, and to track the effectiveness of marketing campaigns, advertising, and affiliate programmes. Usually placed by advertising networks. They may use these cookies to track users across other websites.

(c) Purpose of the Cookies - including whether they can be used for the benefit of another organisation – which appointment must fulfil the conditions set out in clause 5.4(i) above;

(d) Cookies' specific duration; and

(e) Whether the Cookies collect personal data – please note IP addresses and hashed email addresses are personal data.

5.14 If the Supplier fails to comply with the provisions of this Clause 5 then it shall notify John Lewis in writing of any failure to comply within 24 hours of the Supplier becoming aware of such failure to comply. The Supplier shall on demand fully and effectively indemnify, keep indemnified, defend and hold harmless John Lewis and each member of John Lewis Group and their respective directors, officers, agents, employees, successors and assigns from any and all losses, including all claims, expenses, damages, proceedings, costs, and other liabilities resulting from or in connection with any failure to comply with the provisions of this Clause 5 by the Supplier, its Staff, Sub-contractors, third party agents, contractors and associated persons.

6 Information Security Standards

During the Term, the Supplier shall act in accordance with the Information Security Standards, including with regards to Cookies, set out in Appendix 1.

7 Announcements

The Supplier shall not without John Lewis' prior written consent in any way advertise or publicly announce that it is undertaking or has undertaken work for or provided Goods and/or Services to John Lewis.

8 Indemnity and limitation of liability

8.1 The Supplier shall indemnify, keep indemnified and hold John Lewis harmless from any and all losses, liabilities, costs, expenses, proceedings and damages (including, but not limited to, legal and other professional expenses on a full indemnity or solicitor and client basis), arising from or in connection with:

(a) any claim made against John Lewis for actual or alleged infringement of a third party's Intellectual Property Rights arising out of, or in connection with, the Supplier's Pre-existing IPR, the Foreground IPR, the manufacture, supply or use of the Goods, or receipt, use or supply of the Services;

(b) any claim made against John Lewis by a third party for death, personal injury or damage to property arising out of, or in connection with, defects in Goods, to the extent that the defects in the Goods are attributable to the acts or omissions of the Supplier, its staff, agents or sub-contractors;

(c) any damage or destruction to any John Lewis premises or to any John Lewis property to the extent that such damage or destruction is attributable to the acts or omission of the Supplier, its staff, agents or sub-contractors;

(d) any failure to comply with the provisions of Clause 3 (Confidentiality);

(e) any failure to comply with the provisions of Clause 5 (Data Protection);

(f) any failure to comply with the provisions of Clause 24 (Bribery, Corruption and Financial Crime); and

(g) a breach by the Supplier of any law or any breach of the obligations of the Supplier which causes or contributes to any breach of law by any member of the John Lewis Group.

8.2 Subject to Clauses 8.3 and 8.4, the Supplier's total liability to John Lewis arising out of or in connection with this Agreement whether arising in contract, tort (including negligence), breach of statutory duty or otherwise shall be limited in each Contract Year (as defined in Clause 8.6 below) of the Term to the greater of 200% of the Charges paid or payable in that Contract Year and £1,000,000 (one million pounds sterling).

8.3 Nothing in this Agreement excludes or limits the liability of either party in respect of:

(a) death or personal injury caused by its negligence (including negligence of its staff, agents or contractors);

(b) fraud or fraudulent misrepresentation;

(c) any indemnity given by it in this Agreement; or

(d) liability which may not otherwise be limited or excluded by law.

8.4 Subject to Clause 8.3, neither party will be liable to the other party, whether in contract, tort (including negligence), breach of statutory duty or otherwise, for any indirect or consequential loss arising under or in connection with this Agreement.

8.5 Subject to Clauses 8.3 and 8.4, John Lewis' total liability to the Supplier arising out of or in connection with this Agreement whether arising from contract, tort (including negligence), breach of statutory duty or otherwise shall be limited in each Contract Year of the Term to 100% of the Charges paid or payable by John Lewis to the Supplier under this Agreement in that Contract Year. For the avoidance of doubt, any Charges properly due and payable by John Lewis to the Supplier in accordance with this Agreement shall be carved out from John Lewis' limit on liability set out in this Clause 8.5.

8.6 In this Agreement, a "**Contract Year**" shall mean each 12 month period of the Term commencing on the Effective Date and each subsequent anniversary of the Effective Date.

9 Insurance

9.1 The Supplier shall, at all times during the Term, take out and maintain with reputable insurers such policies of insurance as may be necessary to insure the Supplier against all manner of risks that might arise out of the acts or omissions of the Supplier, its agents and/or sub-contractors or otherwise in connection with the Supplier's performance of its obligations under this Agreement, and all policies of insurance that a reputable supplier of Goods and/or Services in the same industry as the Supplier would carry, including, without limitation, in respect of the following risks:

(a) all insurance necessary to insure the Goods against all risks (including, but not limited to, the risks of carriage and product liability and risks related to consumer protection legislation or other laws which impose liability as a result of the manufacture, sale or distribution of products) until such time as risk in the Goods passes to John Lewis in accordance with Clause 12;

(b) loss, damage or destruction of any of John Lewis' property under the custody and control of the Supplier;

(c) public liability insurance; and

(d) employer's liability and all other insurances required by law (including all statutory and regulatory requirements).

9.2 Except where otherwise stated, such insurance cover shall be of an amount adequate to cover everything a reasonably prudent supplier would insure when providing Goods or Services similar to those of the Supplier to cover its obligations under this Agreement but shall in no event be less than £2,000,000 (two million pounds sterling) in respect of any one occurrence.

9.3 If requested by John Lewis, the Supplier shall provide John Lewis with documentary evidence of the existence of such insurance policies and of the payment of the relevant premiums.

10 Warranty

10.1 The Supplier warrants, represents and undertakes that at all times:

(a) its obligations under this Agreement shall be performed with all reasonable diligence, skill and care, and in accordance with the Goods and Services specification and otherwise in accordance with best industry practice and this Agreement (and, in the event that there is any conflict between these standards, the higher standard shall prevail);

(b) all Goods shall be free from all encumbrances and shall be of satisfactory quality (within the meaning of the Sale of Goods Act 1979 as amended) and fit for any purpose held out by the Supplier or made known to the Supplier by John Lewis or of which the Supplier was or should have reasonably been aware, and in this respect John Lewis relies on the Supplier's skill and judgement;

(c) all Goods shall be free from defects in design, material and workmanship and remain so for 12 months after delivery of the Goods or as otherwise agreed in writing between the parties;

(d) it shall comply with all applicable statutory and regulatory requirements relating to the provision of the Goods and Services, including any applicable codes of practice having the force of law or otherwise;

(e) it shall ensure that all of its staff (including any sub-contractors or consultants) perform this Agreement without causing any damage to John Lewis business, public image, reputation and goodwill;

(f) each of its staff (including any sub-contractors or consultants) is suitably qualified, adequately trained, holds appropriate professional qualifications, is lawfully able to work in the UK, and is capable of providing the applicable services in respect of which they are engaged;

(g) the Employment Standards Questionnaire and the Information Security Questionnaire, as applicable, are complete, true and accurate and will remain so throughout the Term; and

(h) the Goods and Services and John Lewis' use of such Goods and Services shall not infringe the Intellectual Property Rights or other rights of any third party or contain any material which is defamatory, libellous, which breaches any rights of privacy or which is otherwise unlawful or illegal.

11 Delivery and Acceptance

11.1 Subject to and without limitation or prejudice to Clause 11.2, John Lewis shall not be deemed to have accepted any Goods until John Lewis has issued a notice in writing confirming its acceptance of such Goods.

11.2 If any Goods delivered to John Lewis do not comply with Clause 10.1, or any other terms of this Agreement, then, without limiting its other rights or remedies, John Lewis shall have one or more of the following rights, whether or not it has accepted the Goods and/or Services:

(a) in respect of the Goods, reject the Goods (in whole or in part) whether or not title has passed and to require the Supplier to remove and replace the rejected Goods at the Supplier's risk and expense within five days of being requested to do so or within such shorter time as John Lewis may specify;

(b) in respect of the Goods, require the Supplier to repair or replace the rejected Goods, or to provide a full refund of the rejected Goods (if paid);

(c) in respect of the Services, at the Supplier's expense, require the Supplier to carry out any additional work as is necessary to correct the Supplier's failure to provide the Services;

(d) recover from the Supplier any expenditure incurred by John Lewis in obtaining substitute goods and/or services from a third party; and

(e) claim damages for any costs, expenses or losses resulting from the Supplier's delivery of Goods or Services that are not in conformity with the terms of this Agreement.

11.3 The Supplier shall deliver the Goods and/or Services in accordance with the terms of this Agreement and to the address instructed by John Lewis, unless otherwise advised in writing by an authorised representative of John Lewis.

11.4 If the Goods and/or Services are not delivered or performed by the applicable date, then, without limiting its other rights or remedies, John Lewis shall have one or more of the following rights:

(a) where John Lewis has paid in advance for the Goods or Services that have not been

provided or delivered by the Supplier, have such sums refunded by the Supplier;

(b) in relation to Goods, refuse to take any subsequent attempted delivery of such Goods;

(c) obtain substitute goods and/or services as applicable from another supplier and recover from the Supplier any costs and expenses reasonably incurred by John Lewis in obtaining such substitute goods and/or services; and

(d) claim damages for any additional costs, loss or expenses incurred by John Lewis which are in any way attributable to the Supplier's failure to meet such obligations.

11.5 The rights and remedies of the parties in connection with this Agreement are cumulative and, except as expressly stated in this Agreement, are not exclusive of any other rights or remedies provided by this Agreement, law, equity or otherwise. For the avoidance of doubt, John Lewis' rights and remedies under this Clause 11 are in addition to the rights and remedies implied into this Agreement by the Sale of Goods Act 1979.

11.6 Except as expressly stated in this Agreement (or in law or in equity in the case of rights and remedies provided by law or equity) any right or remedy may be exercised wholly or partially from time to time.

12 Title and Risk

12.1 The risk in the Goods delivered to John Lewis shall pass to John Lewis on delivery, which shall mean on completion of unloading the Goods at the location specified by John Lewis or as otherwise agreed between the parties in writing.

12.2 Title (with full title guarantee, free from all or any encumbrances and third party rights) to the Goods shall pass to John Lewis on the earlier of (i) payment by John Lewis for the Goods, or (ii) the date the Goods are delivered to John Lewis.

13 Supplier Conduct

13.1 The Supplier shall ensure that all staff, suppliers and sub-contractors assigned to work under this Agreement comply with:

(a) the Modern Slavery Act 2015;

(b) the Health & Safety at Work Act 1974 (as amended) and all applicable laws regarding health and safety;

(c) the John Lewis Policies, as amended by John Lewis by notice from time to time, and any other policies (including, without limitation, any store or site specific policies) notified to the Supplier from time to time; and

(d) all other relevant acts, regulations, statutes, laws and all reasonable instructions and/or requests issued by John Lewis from time to time.

13.2 The Supplier shall be responsible for the training of personnel to perform the Services and ensuring that they conform to the standards of hygiene, discipline and security that apply to John Lewis staff.

13.3 John Lewis may require the Supplier to withdraw any person (whether employed by the Supplier or not) from working on John Lewis' premises.

13.4 The Supplier will notify John Lewis as soon as it becomes aware of:

(a) any health and safety hazards or issues which arise in connection with the performance of this Agreement; and

(b) any breach, or potential breach, of any provision of the John Lewis Policies.

13.5 The Supplier shall implement due diligence procedures for its own suppliers, permitted sub-contractors and other participants in its supply chains, to ensure that there is no slavery or human trafficking in its supply chains.

14 Termination and Consequences of Termination

14.1 The provisions of this Clause 14 are without prejudice to any other rights and remedies of either party under this Agreement or at law.

14.2 John Lewis may terminate this Agreement on written notice to the Supplier in the following situations:

(a) in accordance with Clause 18.2;

(b) at any time and for whatever reason in its sole discretion, by giving at least 28 days' written notice to the Supplier;

(c) by giving at least 7 days' written notice to the Supplier if the Supplier commits a material breach of its obligations under this Agreement which is not capable of remedy or, where capable of remedy, does not remedy such material breach within 14 days of written notice given to it by John Lewis specifying such breach and requiring its remedy;

(d) immediately by notice in writing to the Supplier if the Supplier suffers a change of control as that term is defined in sections 1124 of the Corporation Tax Act 2010; or

(e) if the Supplier does, or omits to do, anything which will cause adverse publicity about John Lewis or will weaken the public image and reputation of John Lewis, by giving at least 7 days' written notice to the Supplier.

14.3 Either party may terminate this Agreement immediately by notice in writing to the other if the other party is subject to an Insolvency Event, which for the purposes of this Agreement means where:

(a) the other party proposes or enters into any composition, compromise or other arrangement for the benefit of its creditors or a class of creditors;

(b) the other party obtains a moratorium or other protection from its creditors;

(c) any person takes any steps towards (1) winding up (where such step is a winding up petition, it shall only constitute an Insolvency Event where such petition is not withdrawn within sixty (60) days) or dissolving the other party (2) appointing a trustee, supervisor, receiver, liquidator, administrator or similar officer or other encumbrancer in respect of the other party or any of its assets and/or (3) taking possession of or levying a distress or execution against any of the other party's assets;

(d) an event occurs which would result in a floating charge crystallising over any of the other party's assets;

(e) the other party stops carrying on business;

(f) the other party is unable to pay its debts or admits it is unable to do so (within the meaning of section 123 of the Insolvency Act 1986 (without any need for the terminating party to prove it in court));

(g) the value of the other party's assets are at any time less than the amount of its liabilities, taking into account its contingent and prospective liabilities; or

(h) any event analogous to any of the above happens in any jurisdiction.

14.4 The Supplier may terminate this Agreement by giving at least 7 days' written notice to John Lewis if John Lewis commits a material breach of the terms of this Agreement and (if such breach is remediable) fails to remedy the material breach within 14 days of receipt of notice in writing to do so.

14.5 Immediately on termination or other expiry of this Agreement the Supplier shall return to John Lewis all equipment, materials, Confidential Information and property supplied to it in connection with this Agreement and the licences granted by John Lewis under Clauses 4.3 and 4.5 shall cease and the Supplier shall have no further right to use John Lewis' Intellectual Property Rights.

15 Employees

15.1 In the event that at any time the Transfer of Undertakings (Protection of Employment) Regulations 2006, as amended or replaced, (the "**Transfer Regulations**") operate or are alleged to operate to transfer the employment of any employee or worker in connection with the Agreement or the Services to be provided hereunder, the Supplier will (without limitation) indemnify and keep indemnified on an ongoing basis John Lewis, any member of the John Lewis Group and any other supplier that takes over the provision of the same or similar services (a "**Successor**"), against any and all Employment Liabilities (as defined in Clause 15.3) that John Lewis, any member of the John Lewis Group or the Successor may incur as a result of or in connection with any such operation or alleged operation of the Transfer Regulations (or otherwise), howsoever or whenever such Employment Liabilities arise. For the avoidance of doubt this includes, without limitation:

(a) all Employment Liabilities relating to the dismissal or alleged dismissal of any employee or worker of the Supplier or any sub-contractor (whether such dismissal is effected by John Lewis, the Supplier, any sub-contractor, any Successor or otherwise) or any other liability which John Lewis, any member of the John Lewis Group or any Successor inherits/could inherit under the Transfer Regulations; and

(b) any liability (howsoever arising) for any failure or alleged failure of any person (including without limitation John Lewis, any member of the John Lewis Group, the Supplier, any sub-contractor and any Successor) to comply with the Transfer Regulations.

15.2 Further, the Supplier shall (and shall procure that any sub-contractor shall) give to John Lewis, any member of the John Lewis Group or the Successor such co-operation or assistance as John Lewis may reasonably require in relation to any of its or their employees or workers who provide the Services (including, without limitation, the provision of such accurate written information as John Lewis requires in respect of such employees or workers) and shall promptly comply with any lawful instruction issued by John Lewis in relation to such employees or workers.

15.3 For the purposes of Clause 15.1 above "**Employment Liabilities**" means any costs, claims, demands, fines, or expenses (including legal and other professional expenses), payments, wages, actions, proceedings, compensation, awards, interest, loss, damages or penalties howsoever arising including but not limited to any redundancy costs (including any notice pay, holiday pay and any statutory and contractual redundancy payments) and any liabilities for income tax to be collected through the Pay As You Earn Scheme and any primary and secondary National Insurance contributions.

16 Audit and Reporting

16.1 The Supplier shall maintain complete and accurate records and supporting documentation relating to the performance of its obligations under this Agreement.

16.2 The Supplier shall promptly make available to John Lewis, on John Lewis' request, all and any information necessary for monitoring the Supplier's performance.

16.3 The Supplier shall allow on reasonable notice any of John Lewis' staff and its internal and external auditors access to such information as may in the opinion of John Lewis be necessary for audit purposes and John Lewis may take copies of any such information.

17 Assignment

17.1 The Supplier may not assign, transfer, mortgage, charge, sub-contract, declare a trust over or deal in any other manner with all or any of its rights under the Agreement without John Lewis' prior written consent, but notwithstanding this if such consent is given, the Supplier shall not be relieved of any of its obligations under the Agreement.

17.2 John Lewis may at any time assign, transfer, mortgage, charge, sub-contract, declare a trust over or deal in any other manner with all or any of its rights or obligations under this Agreement.

18 Force Majeure

18.1 Neither the Supplier nor John Lewis shall be liable for any expense, loss or damage resulting from delay or prevention of performance of the Agreement that is caused by fires, floods, acts of God, riots, thefts, accidents or any other circumstance that is beyond the affected party's control (but excluding for the avoidance of doubt any strikes, lock-outs or industrial action, by the employees, workers or agents of the Supplier) (a "**Force Majeure Event**").

18.2 If the Force Majeure Event prevents, hinders or delays the affected party's performance of its obligations for a continuous period in excess of 28 days, or periods which, when aggregated, are in excess of 28 days, after the date which the Force Majeure Event began, John Lewis shall be entitled to terminate this Agreement immediately on notice to the Supplier.

19 Notices

19.1 Any notice or communication to be given under this Agreement shall be in writing and shall be delivered by hand or sent by pre-paid first class recorded delivery post to the party to be served at that party's registered office (if it is a company) or its principal place of business (in any other case) from time to time marked for the attention of the Company Secretary of that party.

19.2 Any such notice shall be deemed to have been received:

(a) if delivered by hand, at the time of delivery; or

(b) if posted, at 9am on the second business day after posting.

20 Severance

20.1 If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this Clause 20 shall not affect the validity and enforceability of the rest of the Agreement.

21 Waiver

21.1 A waiver of any right or remedy under the Agreement or by law is only effective if given in writing and shall not be deemed a waiver of any subsequent breach or default.

21.2 The failure or delay by John Lewis in exercising any right, power or remedy that it might have under this Agreement or law shall not in any circumstances impair such right, power or remedy nor operate as a waiver of it, nor shall it prevent or restrict the further exercise of that or any other right or remedy. The single or partial exercise by John Lewis of any right, power or remedy under this Agreement shall not in any circumstances preclude any other or further exercise of it or the exercise of any other right, power or remedy.

21.3 Any waiver of a breach of, or default under, any of the terms of this Agreement shall not be deemed a waiver of any subsequent breach or default and shall in no way affect the other terms of this Agreement.

22 Entire Agreement

22.1 This Agreement sets out the entire agreement and understanding between the parties relating to its subject matter.

22.2 Subject to any statements, representations, promises or assurances as to fitness for purpose of Goods or otherwise and any reliance by John Lewis on the Supplier's skill and judgement as set out in Clause 10.1(b), each party acknowledges that it has not relied on any statement, representation, warranty, promise or assurance that is not set out in this Agreement.

23 Rights of Third Parties

23.1 Subject to Clause 23.2 below, a person who is not a party to this Agreement shall have no rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any provisions of this Agreement.

23.2 Notwithstanding Clause 23.1, each member of the John Lewis Group (as that term is defined in Clause 3) shall have the benefit of all rights, benefits, indemnities and limitations provided for in this Agreement and accordingly shall be entitled to enforce this Agreement subject to and in accordance with its terms.

23.3 Any member of the John Lewis Group may receive the Goods and/or Services, and pay the Charges for the Goods and/or Services received, under this Agreement and/or benefit from the Goods and/or Services that have been provided to another member of the John Lewis Group.

24 Bribery, Corruption and Financial Crime

24.1 The Supplier shall:

(a) at all times comply with all applicable Laws and sanctions relating to anti-bribery, corruption and financial crime including but not limited the Bribery Act 2010 (the "**Bribery Act**") and the Criminal Finances Act 2017 (the "**CFA**");

(b) not engage in any activity, practice or conduct which would constitute an offence by it under the Bribery Act or the CFA;

(c) devise, implement and enforce written policies and procedures constituting adequate procedures under the Bribery Act in order to prevent commission of any offence under the Bribery Act and/or any breach of any relevant John Lewis Policies by the Supplier, its Staff and any third party agents, contractors and/or associated persons to the Supplier. The Supplier shall, on John Lewis' request, provide John Lewis copies of such written policies and procedures;

(d) devise, implement and enforce written policies and procedures constituting prevention procedures under the CFA in order to prevent the facilitation of tax evasion and/or commission of any offence under the CFA and/or any breach of any relevant John Lewis Policies by the Supplier, its Staff and any third party agents, contractors and/or associated persons to the Supplier. The Supplier shall, on John Lewis' request, provide John Lewis copies of such written policies and procedures;

(e) promptly report to John Lewis any request or demand for any undue financial or other advantage of any kind received by the Supplier in connection with the performance of this Agreement; and

(f) promptly report to John Lewis if it has or has reasonable grounds to believe it may have committed an offence under the CFA.

25 Non-exclusivity

25.1 Nothing in this Agreement grants the Supplier any exclusivity in the supply of the Goods and Services to John Lewis and John Lewis may procure the supply of the Goods or Services or items similar to the Goods and Services from any third party supplier it wishes at its sole discretion.

25.2 John Lewis shall have no obligation to purchase a minimum quantity of Goods and/or Services under this Agreement and, at its sole discretion may determine not to purchase any Goods and/or Services at all.

26 Variation

26.1 No variation to this Agreement shall be valid unless it is in writing and signed for and on behalf of each of the parties.

27 Survival

27.1 Termination or expiry of this Agreement for any reason shall not affect any rights or liabilities that have accrued prior to such termination or expiry or the coming into force or continuance in force of any term that is expressly or by implication intended to come into or continue in force on or after termination or expiry.

27.2 Without prejudice to the generality of Clause 27.1 where a Clause in this Agreement (including without limitation Clauses 3, 4, 5, 5.1, 8, 10, 14.5, 15, 24, 27 and 28) expressly or impliedly has effect on termination or other expiry of this Agreement, that Clause shall continue in force on and after such termination or expiry.

28 Governing Law and Jurisdiction

28.1 This Agreement and any non-contractual obligations arising out of or in connection with it is governed by and shall be interpreted in accordance with English Law.

28.2 Each party irrevocably submits to the exclusive jurisdiction of the English courts in relation to all matters arising out of or in connection with this Agreement.

29 Counterparts

This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all of which taken together shall constitute one and the same instrument.

Appendix 1

Supplier Information Security Standard ('**SISS**')

(A) This Schedule sets out minimum security requirements expected of Suppliers and other third

parties which will have access to or will process data of the John Lewis Group in the provision of Goods and Services under this Agreement. These are John Lewis's minimum standards.

(B) The Supplier represents to John Lewis that it will comply with this Schedule (or if it is unable to do so immediately, agree with John Lewis to implement a Risk Treatment Plan to ensure future compliance) and John Lewis has relied on those representations on entering into this Agreement.

(C) If there are any queries relating to any of these standards, please contact your John Lewis Representative, or a member of the John Lewis Information Security team.

This Schedule relates to the Supplier identifying and understanding the risks relating to John Lewis data and taking appropriate action to ensure all information security risks are mitigated to acceptable levels. For the avoidance of doubt, John Lewis data includes all data owned, processed or produced by or on behalf of John Lewis.

The Supplier shall:

1 **INFORMATION SECURITY POLICIES**

1.1 **Policies for Information Security**, ensure the Supplier and the Supplier Group has comprehensive policies for information security that are approved by management, published and effectively communicated to all employees and relevant external parties;

1.2 **Review of the Information Security Policy**, ensure the policy has an owner defining responsibility for its maintenance and review according to a defined review process. Ensure the process ensures that a review of supporting procedures and processes is undertaken if the policy changes.

2 **ORGANISATION OF INFORMATION SECURITY**

2.1 **Segregation of duties,** ensure conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the Supplier and Supplier Group's assets;

2.2 **Information security in project management,** ensure information security is addressed in project management methodologies regardless of the type of project;

2.3 **Mobile device policy,** ensure information security is addressed in project management methodologies regardless of the type of project;

2.4 **Teleworking,** ensure there is any policy, procedure and/or standard to control remote working activities. This should be consistent with the Supplier or Supplier Group's security policy. Ensure the teleworking site is protected from theft and unauthorised access.

3 **EMPLOYMENT**

3.1 **Screening**, ensure verification checks on all staff were carried out at the time of job applications. This should include character reference, confirmation of claimed academic & professional qualifications and independent identity checks;

3.2 **Terms and conditions of employment,** ensure terms and conditions of the employment covers the employee's responsibility for information security;

3.3 **Management responsibilities,** ensure managers are aware of their responsibilities with regard to ensuring that established policies and procedures are applied by external parties, contractors and employees;

3.4 **Information security, awareness, education and training,** ensure employees, third parties and contractors receive appropriate awareness training and regular updates in organisational policies and procedures as relevant for their job function;

3.5 **Termination or change of employment responsibilities**, ensure a formal procedure exists for performing all employment terminations or change of employment and assignment of responsibility for this. This includes the requirement to maintain confidentiality after employment ceases and return of assets.

4 **ASSET MANAGEMENT**

4.1 **Inventory of assets,** ensure an inventory or register is maintained for assets associated with each information system including data;

4.2 **Ownership of assets,** ensure a procedure exists to assign asset ownership at the time the asset is created or when assets are transferred to the Supplier or the Supplier Group;

4.3 **Acceptable use of assets,** ensure rules for acceptable use of information and assets associated with information processing are documented and implemented;

4.4 **Classification of information,** ensure there is an information classification scheme or guideline in place which will assist in determining how the information is to be handled, protected and labelled;

4.5 **Management of removable media,** ensure there exists a procedure for management of removable media, including encryption of devices, in all its forms particularly the use of devices that plug into a USB port. This includes backup media and CDs, DVDs and portable hard drives;

4.6 **Disposal of media,** ensure media that is no longer required is disposed off securely and safely. Ensure the disposal of confidential items is logged where necessary in order to maintain an audit trail.

5 **ACCESS CONTROL**

5.1 **Access Control Policy,** ensure asset owners have determined appropriate access control rules, access rights and restrictions for specific user roles. The strictness of the access rules must reflect the associated information security risks;

5.2 **Access to networks and network services,** ensure users are only able to gain access to the network (e.g. specific shares, menus etc.) or network services that they have been specifically authorised to use;

5.3 **User registration and de-registration,** ensure the Supplier and the Supplier Group has a formal registration and de-registration procedure and documents where shared user IDs have been approved;

5.4 **User access provisioning,** ensure there is a documented procedure for approving and setting up user access in accordance with access control policies. This should be based on job role requirements;

5.5 **Management of privileged access rights,** ensure the allocation and use of any privileges in multi-user information system environment is restricted and controlled e.g. Privileges are allocated on need-to-use basis; privileges are allocated only after formal authorisation process;

5.6 **Management of secret authentication information of users**, ensure the allocation and reallocation of secret authentication information e.g. passwords should be controlled through a formal management process, including maintain secure passwords. Ensure the users are asked to sign a statement to keep this information confidential;

5.7 **Review of user access rights**, ensure there exists a process to review user access rights at regular intervals e.g. Special privilege review every 3 months, normal privileges every 6 months;

5.8 **Secure log on procedures,** ensure access to information system is attainable only via a secure log-on process, the default access being none. Consider enabling multi-factor authentication for access to confidential information from an untrusted network and for privileged access to information systems;

5.9 **Password management system,** ensure there exists a password management system that enforces various password controls such as individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc.;

5.10 **Access to program source code,** ensure there are controls in place to prevent the introduction of unauthorised functionality, unintentional changes and to maintain the confidentiality of valuable intellectual property.

6 **CRYPTOGRAPHY**

6.1 **Policy on the use of cryptographic controls,** ensure there is an up-to-date Policy in place for the use of cryptographic controls for protection of confidential or secret information;

6.2 **Key Management;** ensure there is a management system is in place to support the Supplier Group's use of cryptographic techniques such as secret key technique and public key techniques. Ensure the Key management system is based on agreed set of standards and procedures.

7 **PHYSICAL AND ENVIRONMENTAL SECURITY**

7.1 **Physical security perimeter**, ensure physical security facilities have been implemented to protect the Information processing service. Some examples of such security facility are card control entry gate, walls, manned reception etc.;

7.2 **Physical entry controls,** ensure entry controls are in place to allow only authorised personnel into various areas within the Supplier Group's premises;

7.3 **Working in Secure areas**, ensure there exists any security controls for third parties or for personnel working in secure area;

7.4 **Delivery and loading area,** ensure the delivery and loading areas are isolated and secure to prevent unauthorised access to information processing facilities;

7.5 **Equipment sitting and protection** ensure the equipment is located to minimise unnecessary access into work areas. Ensure the items requiring special protection were isolated to reduce the general level of protection required including those relating to environmental threats;

7.6 **Secure disposal or reuse of equipment,** ensure equipment or media is verified to certify that any confidential information, data or software is removed prior to disposal or reuse;

7.7 **Clear desk and clear screen policy,** ensure automatic computer screen locking and password protected screen savers are enabled, as well as user's responsibility to implement such protection for unattended equipment.

8 **OPERATIONS SECURITY**

8.1 **Change management,** ensure change management controls have been implemented to ensure satisfactory control of all changes including changes to software development in-house and software packages;

8.2 **Separation of development, testing and operational environments,** ensure the development and testing facilities are isolated from operational facilities e.g. development software should run on a different computer to that of the computer with production software. Development and production networks should be separate;

8.3 **Controls against malware,** ensure adequate detection, prevention and recovery controls to protect against malware are implemented and combined with a high level of user awareness;

8.4 **Information backup**, ensure backups of essential business information e.g. production server, critical network components, configuration etc are taken regularly Ensure the backup media along with the restore procedure are stored securely and well protected;

8.5 **Event logging,** ensure systems are configured for recording user activities, exceptions, faults and information security events;

8.6 **Protection of log Information,** ensure log information and audit trails are adequately protected by security controls to prevent tampering;

8.7 **Log aggregation and Monitoring,** ensure that event logs are transmitted to a log aggregation

system and there is a process for monitoring event logs;

8.8 **Administrator and operator logs,** ensure system administrator and system operator activities are logged and the logs protected and regularly reviewed;

8.9 **Management of technical vulnerabilities,** ensure the Supplier Group subscribes to any alerting services or receives advisory information about technical vulnerabilities and that technical staff use this information to mitigate potential risks to information systems.

9 **COMMUNICATIONS SECURITY**

9.1 **Network controls;** ensure there are controls implemented to ensure the security of information in networks and the protection of connected services from unauthorised access;

9.2 **Security of network services,** ensure security requirements to enable a service provider to manage agreed services in a secure way have been determined and regularly audited and monitored;

9.3 **Segregation in networks,** ensure the network is segregated appropriately to facilitate effective information security. This may relate to separate network domains based on entity, location, workgroup or technology considered less trusted;

9.4 **Information transfer policies and procedures,** ensure there are procedures and controls in place to protect the transfer of information and ensure staff are reminded to maintain the confidentiality of information while using technology such as email, phones, fax and voicemail;

9.5 **Electronic messaging,** ensure there is a policy in place for the acceptable use of email, instant messaging and other electronic communications.

10 **SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**

10.1 **Information security requirements analysis and specification,** ensure information security related requirements are included in the requirements for new information systems or enhancements to existing information systems;

10.2 **Securing application services on public networks,** ensure information involved in application services passing over a public network is well protected from fraudulent activity, contract dispute and disclosure or modification of information;

10.3 **Secure development policy,** ensure security has been integrated in all phases of software development and documented in a secure development policy;

10.4 **Technical review of applications after operating platform changes,** ensure there are process or procedure in place to ensure application systems are reviewed and tested after changes to the operating system;

10.5 **Secure system engineering principles,** ensure principles and procedures for engineering secure systems have been established, documented, maintained and applied to any information system implementation efforts;

10.6 **Secure development environment**, ensure the Supplier Group has appropriately assessed the risks associated with individual system development and integration efforts that cover the entire system development lifecycle;

10.7 **Outsourced development,** ensure there are controls in place over outsourcing software. The points to be noted includes: Licensing arrangements, escrow arrangements, contractual requirement for quality assurance, testing before installation to detect malware;

10.8 **System security testing,** ensure a procedure for testing is included in software development projects including test inputs and expected outputs under a range of conditions and ensure this is appropriate to the criticality of the application. In addition, consider independent penetration testing for critical applications;

10.9 **System acceptance testing**, ensure acceptance testing programs have been established for new information systems, upgrades and new versions;

10.10 **Protection of test data,** ensure system test data is protected and controlled. The use of operational database containing personal information should be avoided for test purposes. If such information is used, the data should be depersonalised before use;

11 **SUPPLIER RELATIONSHIPS**

11.1 **Information security policy for supplier relationships,** ensure there is a policy for addressing supplier access to the Supplier Group's information based on the Supplier Group's access control criteria;

11.2 **Addressing security within supplier agreements,** ensure the requirements for security have been established and agreed with individual suppliers that may access, process, store, communicate or provide IT infrastructure components for the Supplier Group's information, including monitoring and auditing;

11.3 **Information and communication technology supply chain,** ensure documented agreements with suppliers include requirements to address information security risks associated with the information and communications technology services and product supply chain.

12 **INFORMATION SECURITY INCIDENT MANAGEMENT**

12.1 **Responsibilities and procedures,** ensure management responsibilities and procedures have been established to ensure a quick, effective and orderly response to information security incidents, within defined timeframes in the GDPR;

12.2 **Reporting information security weaknesses,** ensure a formal reporting procedure or guideline

exists for users, to report security weakness in, or threats to, systems or services;

12.3 **Assessment of and decision on information security events,** ensure there is a procedure for assessing information security problems and issues and classifying them as information security incidents;

12.4 **Response to information security incidents,** ensure there are documented procedures in place for responding to an information security incident including report security incidents through appropriate management channels as quickly as possible.

13 **COMPLIANCE**

13.1 **Independent review of information security,** ensure policies, processes, procedures, controls and control objectives are subject to regular independent reviews at planned intervals or when significant changes occur;

13.2 **Compliance with security policies and standards,** ensure information systems were regularly checked for compliance with security implementation standards by Managers;

13.3 **Technical compliance review,** ensure technical security reviews are carried out either manually or using automated tools to confirm information security objectives are achieved - e.g. penetration testing and vulnerability assessments.

14 **TECHNICAL**

14.1 **Inventory of authorised and unauthorised devices,** maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device;

14.2 **Inventory of authorised and unauthorised software,** devise a list of authorised software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorised software has not been modified;

14.3 **Secure configurations for hardware and software,** establish standard secure configurations of your operating systems and software applications. Standardised images should represent hardened versions of the underlying operating system and the applications installed on the system;

14.4 **Email and web browser protections,** ensure that only fully supported web browsers and email clients are allowed to execute in the organisation, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes;

14.5 **Limitation and control of network ports,** ensure that only ports, protocols, and services with validated business needs are running on each system. Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed;

14.6 **Secure configurations for network devices,** compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the Supplier Group. The security configuration of such devices should be documented, reviewed, and approved by a change control board in the Supplier Group;

14.7 **Boundary defence,** deny communications with (or limit data flow to) known malicious IP addresses (blacklists), or limit access only to trusted sites (whitelists);

14.8 **Wireless access control,** ensure that each wireless device connected to the network matches an authorised configuration and security profile, with a documented owner of the connection and a defined business need;

29.1 **Application software security,** for all acquired application software, the version you are using must be supported by the vendor. If not, you must update to the most current version and install all relevant patches and vendor security recommendations.