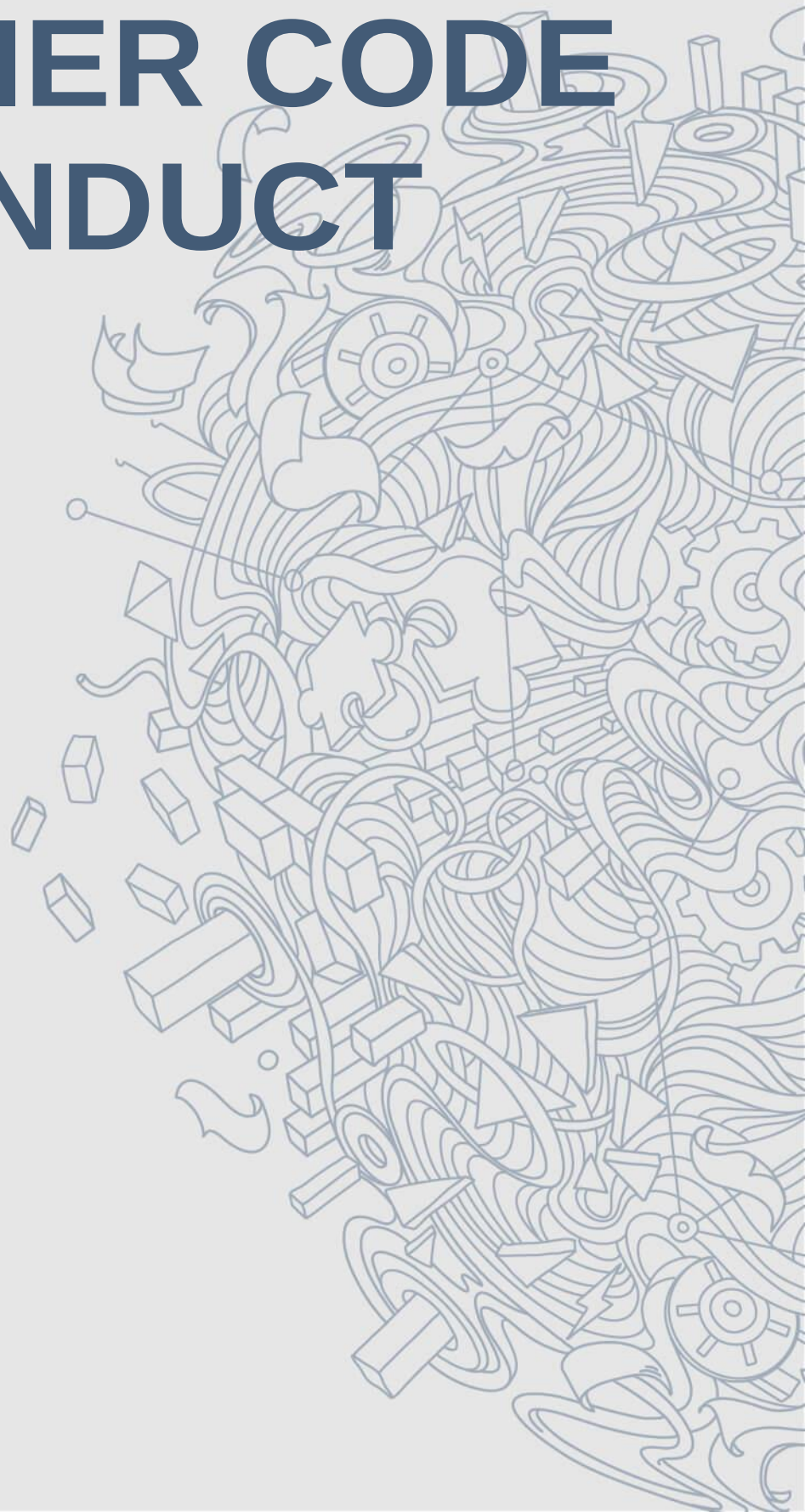
# PROCUREMENT POLICY & SUPPLIER CODE OF CONDUCT

AG Procurement



ADDLESHAW GODDARD

# THE PROCUREMENT POLICY

The Procurement Policy and Supplier Code of Conduct, in conjunction with the firm's Business with Integrity Statement, provide detail about the Addleshaw Goddard ethos, our aspirations for how our business operates and the expectations we have of our suppliers. It is integral to our business strategy and success that we have a positive impact when dealing with our clients, suppliers, employees and wider society wherever we do business.

As such, the Procurement Policy describes the firm's commitment to ensuring that all procurement activities carried out by the firm are conducted in an honest, competitive, fair and transparent manner, and that incumbent suppliers are appropriately managed on an ongoing basis. The firm employs The AG Procurement Standard as a set of internal rules for those involved in procurement activity, to support this commitment.

The AG Procurement Team consider a variety issues when evaluating potential suppliers over and above service delivery and cost, including: risk management, statutory and regulatory compliance, corporate social responsibility, diversity, sustainability and environmental credentials, and innovation.

We pledge to:

- Conduct our procurement activity with integrity at all times,
- Deliver value for money outcomes for the firm, in an ethical and sustainable way,
- Appropriately manage a range of supplier-related risks,
- Build relationships with preferred suppliers who understand our business needs,
- Ensure supplier diversity and effective supplier management approaches are employed,
- Seek out innovation and collaboration within our supplier base, and
- Protect the reputation and meet the regulatory requirements of the firm with regard to procurement activity and supplier engagement.

Addleshaw Goddard is committed to working with our suppliers to ensure that the principles set out in our Procurement Policy and Standard are met by the firm, and that the Supplier Code of Conduct is adhered to by all of the firm's suppliers and throughout the supply chain.

# THE SUPPLIER CODE OF CONDUCT

## INTRODUCTION

The Supplier Code of Conduct sets out our expectations of suppliers, generally in terms of business practices, and specifically with regard to:

- ethical supply and people practices including diversity and inclusion,
- prevention of financial crime,
- environmental responsibility,
- data protection and information security,
- health and safety.

Addleshaw Goddard procures goods and services from a large number of suppliers, internationally, and the firm recognises that each supplier may have their own standards and ambitions for the above. We expect all of our suppliers to meet the requirements set out in legislation, regulation, and good industry practice and to ensure that their suppliers do the same.

In combination, the Addleshaw Goddard Procurement Policy and Supplier Code of Conduct set out the commitments from the firm and expectations of our suppliers, and the results we aim to achieve by working together. No organisation that shares our values should be precluded from working with Addleshaw Goddard. Working together across our supply chains, we will encourage and enable sustainability and long-term positive impacts on the global community.

The Procurement Policy and Supplier Code of Conduct is reviewed periodically (annually as a minimum), and will be revised as necessary to ensure that this document helps us become a more sustainable business, delivering continuous improvement for our clients, our stakeholders and the communities in which we operate.

Changes to the Supplier Code of Conduct will be notified to all suppliers from time to time and all suppliers shall comply with new requirements that are relevant to their business, as soon as practicable.

# GENERAL REQUIREMENTS

**1 General requirements for all suppliers**

1.1 Addleshaw Goddard expects its suppliers to behave ethically, apply high standards of corporate conduct and to fully comply with all relevant law.

1.2 Addleshaw Goddard has a zero tolerance approach to improper business conduct of any sort and all our suppliers are required to confirm that their business practices meet the standards set out in this Supplier Code of Conduct, as a minimum.

**2 General Requirements for prospective suppliers**

2.1 Prospective suppliers shall keep all pre-contract data, negotiations and tender progress strictly confidential and shall, at our request, enter into a more detailed non-disclosure agreement.

2.2 Prior to entering into any contract, Addleshaw Goddard carries out due diligence on each supplier in order to comply with relevant law and to assess suitability of the supplier to meet our business needs. Suppliers must co-operate fully and promptly with due diligence enquiries. Suppliers shall be required, at the discretion of and where deemed appropriate by Addleshaw Goddard, to propose exit plans, business continuity plans, disaster recovery plans and/or other similar documents when entering into contract or where tendering, in order that the firm can appropriately plan for and mitigate against potential future issues.

2.3 All activity between Addleshaw Goddard and potential suppliers will be conducted with integrity. Contracts will be awarded based on merit. Hospitality or other inducements which seek to encourage or reward a decision must not be offered to our employees or any other individuals associated with Addleshaw Goddard. The acceptance of gifts, hospitality or inducements of any nature during a competitive tender by our employees is strictly prohibited.

**3 General requirements for current suppliers**

3.1 Where Addleshaw Goddard enters into a contract with a supplier, the relationship will be governed by agreed terms and conditions. In addition, the supplier shall comply with the requirements of this Supplier Code of Conduct only to the extent that such requirements are:

(a) not already expressly agreed in the contract between us; and

(b) relevant to the supplier and/or the services being provided, given all the circumstances.

3.2 As part of supplier management, Addleshaw Goddard carries out due diligence on each supplier in order to ensure compliance with relevant law and to ensure the supplier continues to meet our business needs. Suppliers must cooperate fully and promptly with due diligence enquiries. From time to time, suppliers may be required, at the discretion of and where deemed appropriate by Addleshaw Goddard, to propose exit plans, business continuity plans, disaster recovery plans and/or other similar documents, in order that the firm can appropriately plan for and mitigate against potential future issues.

3.3 It is recommended that suppliers' policies and procedures are reviewed regularly to ensure that changes in regulations, technology, and industry best practice are captured, as well as changes within the organisation. Regular review will ensure that sound governance is encouraged and instilled which will demonstrate continuous improvement.

3.4 Suppliers are encouraged to support Addleshaw Goddard's Corporate Social Responsibility activities, please click here for further information.

**4 Ethical Supply – people practices**

4.1 Suppliers shall respect the human rights of their employees, other personnel and local communities and shall comply with all relevant law pertaining to human rights.

4.2 Addleshaw Goddard is taking steps to identify and eradicate modern slavery in its business and supply chain. Suppliers shall also take appropriate steps to identify and eradicate modern slavery, in all its forms, including slavery, servitude, forced and compulsory labour and human trafficking, whether of adults or children, all forms of which have in common the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain.

4.3 We are also committed to ensuring there is transparency in our approach to tackling modern slavery throughout our supply chains, consistent with our disclosure obligations under the Modern Slavery Act 2015. We expect the same commitment from all our suppliers and we expect that our suppliers will hold their own suppliers to the same high standards.

4.4 Suppliers shall implement appropriate due diligence practices and provide training to identify the risk of and/or actual instances of modern slavery.

4.5 Suppliers shall document all the steps taken to tackle modern slavery and shall, on request, provide a report to Addleshaw Goddard setting out all policies and procedures implemented, including due diligence undertaken, risk areas identified, how risks have been mitigated, training provided and consequences for third parties of non-compliance.

4.6 All suppliers shall ensure that, within their own organisations and throughout the supply chain:

(a) child labour shall not be used and relevant law pertaining to minimum working age legislation shall be strictly complied with;

(b) forced labour, in any form, shall not be used and supplier workers shall not be required to lodge papers or deposits on starting work; and

(c) physical abuse, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation or inhumane practice shall not take place, whether as part of a disciplinary process or otherwise, and shall be prohibited.

4.7 Addleshaw Goddard is committed to a policy of equality opportunity in our employment practices in order to ensure that no job applicant, employee or any other individual is discriminated against and less fairly treated because of gender identity or marital status, race (including nationality or ethnic origin), disability or any health condition, religion, age, sexual orientation, union membership, political affiliation, being a member of a protected class under international human rights law or any other conditions not justified in relevant law or relevant to the performance of the job.

4.8 Addleshaw Goddard is committed to creating an inclusive workplace where individuals are able to be themselves, irrespective of their gender identity, race (including nationality or ethnic origin), disability or any health condition, religion, age and sexual orientation. As such, we expect our suppliers to be committed to the same principles and require them to have policies in place to promote diversity and inclusion within their own organisations and supply chain, including, but not limited to work place standards such as the Disability Confident Scheme or equivalent. Further, we expect suppliers to agree to provide evidence of their commitment upon reasonable request.

4.9 All terms and conditions of employment must be made clear to the workforce in a manner which is easily understood by that workforce. The supplier shall ensure that:

(a) employee wages comply with relevant law pertaining to the minimum wage and that minimum wage or the prevailing industry wage (whichever is higher) shall be paid to workers as a minimum;

(b) each employee shall be provided with all benefits under relevant law and no non-statutory deductions shall be made from wages;

(c) the employment terms of young workers must adhere to International Labour Organisation Standards, the OECD Guidelines for Multinational Enterprises and relevant law;

(d) relevant law pertaining to working time and the maximum hours of work permitted to be undertaken by any employee in any period of time, must be complied with, and any overtime shall be on a voluntary basis and at manageable levels;

(e) all employees, whether local or migrant, have the right and ability to leave employment when they choose; and

(f) obligations to direct employees under relevant law arising from regular employment shall not be avoided through the use of labour-only contracting, sub- contracting, or home-working arrangements, or through apprenticeship schemes where there is no real intent to impart skills or provide regular employment, nor shall any such obligations be avoided through the excessive use of fixed-term contracts of employment.

4.10 Suppliers must provide workers with clear, fair and uniformly applied disciplinary practices and grievance procedures.

4.11 Supplier shall recognise the rights of workers to form or join trade unions which are free to meet without hindrance and to bargain collectively. Suppliers shall adopt an open attitude towards the activities of trade unions and where it is not practicable for unions to operate, recognise other means of association, such as Works Councils.

4.12 Training, including that required under relevant law and industry specific training (whether mandatory or best practice) shall be provided to workers and regular refresher training provided on a timely basis.

4.13 Suppliers shall provide sufficient evidence, promptly upon on request from Addleshaw Goddard, that they have implemented appropriate procedures to manage all labour related issues within their supply chain to ensure that they comply with relevant law and this Code of Conduct.

4.14 Suppliers shall demonstrate, through supply chain transparency, that people are dealt with ethically and lawfully and that goods are traded fairly and meet the environmental aims detailed in this Code of Conduct.

**5 Prevention of Financial Crime**

5.1 In this section, Financial Crime shall include bribery, corruption, money laundering, terrorist financing, tax evasion and the failure to prevent the criminal facilitation of tax evasion.

5.2 Suppliers shall comply with all relevant law pertaining to Financial Crime and shall not do or omit to do anything which would cause Addleshaw Goddard to be in breach of such relevant law.

5.3 With regard to anti-bribery and anti-corruption measures, suppliers shall put in place an appropriate policy and procedures which prohibit workers from:

(a) the offering, giving, soliciting or receiving of a bribe at any time (including the making of facilitation payments or the bribery of public officials) whether for the benefit of the supplier or for the benefit of the worker, a member of the worker's family, friends, associates or acquaintances;

(b) the use of a gift or hospitality to induce a fraud or other wrongdoing to secure a personal or business benefit;

(c) the use of sponsorship or advertising agreements to exercise undue influence; or

(d) unapproved or unauthorised charitable donations or political donations of any kind.

5.4 With regard to anti-money laundering and counter terrorist financing measures, suppliers shall put in place an appropriate policy and procedures which:

(a) verify the legitimate origin of goods and services within their supply chain; and

(b) verify the identity and the legitimate nature of the businesses with which the supplier contracts.

5.5 With regard to tax evasion, suppliers shall have adopted a tax strategy that demonstrates a willingness to pay the right amount of tax, in the right place at the right time.

5.6 With regard to measures to prevent the criminal facilitation of tax evasion, suppliers shall put in place an appropriate policy and procedures which:

(a) regularly assess the opportunity, motive and means within their business for the criminal facilitation of tax evasion;

(b) implement reasonable preventative measures by developing procedures that are appropriate to the mitigate the identified risks; and

(c) effectively communicate the expectations of management, being that compliance with such policy and procedures is mandatory and that the business takes a zero-tolerance approach to any breach.

5.7 As part of the prevention, identification and detection of Financial Crime issues, suppliers shall implement mandatory training for workers, appropriate oversight, regular risk assessments, appropriate due diligence and procedural audits.

5.8 Suppliers shall encourage workers to promptly report to an appropriate senior manager if they know of or suspect any business activity that is in contravention of the supplier's Financial Crime procedures, and shall implement disciplinary action for any worker failing to comply with such procedures.

5.9 Suppliers shall make sure that workers do not suffer any adverse consequences for making a report under the Financial Crime policies, whistle-blowing or refusing to pay a bribe, even if such refusal may result in the supplier losing business.

5.10 The supplier shall keep sufficiently detailed records relating to the identification and prevention of Financial Crime and shall promptly notify Addleshaw Goddard upon becoming aware of any instance or suspected instance of Financial Crime connected to the business relationship between Addleshaw Goddard and the supplier.

5.11 Addleshaw Goddard has a responsibility to detect and prevent Financial Crime, accordingly, suppliers shall comply with Addleshaw Goddard procedures, relating to due diligence and the verification of the legitimate nature of:

(a) supplier entities;

(b) payment processes and funding arrangements; and

(c) any other aspects of the goods and service provision by the supplier,

as are notified to the supplier from time to time.

**6 Environmental Responsibility**

6.1 Suppliers shall comply with all relevant law pertaining to the environment and shall operate their business in an environmentally responsible way.

6.2 Suppliers shall take a proactive approach to working with Addleshaw Goddard towards reducing our environmental impact.

6.3 Supplier shall:

(a) adopt such practices and utilise such systems that minimise the use of resources e.g. water efficiency, energy efficiency;

(b) ensure that it and its suppliers use environmentally friendly working practices, tools and equipment, consumables and replacement parts, wherever possible;

(c) ensure where practicable that all consumables originate from a sustainable or recycled source;

(d) ensure there are facilities or arrangements in place, either directly or through its suppliers to ensure we can return used packaging for recycling, reuse or environmentally friendly disposal; and

(e) ensure that any hazardous or toxic waste that is produced must be properly identified and disposed of by licensed and competent bodies via authorised and/or licensed means.

6.4 Suppliers shall have a written environmental / sustainability policy appropriate to the size and nature of their operation which addresses preventing, mitigating and controlling serious environmental and health impacts from their operations. This policy will be:

(a) reviewed annually;

(b) signed and dated by senior management; and

(c) provided to Addleshaw Goddard on request.

6.5 Each supplier shall carry out annual reviews and audits of its environmental performance and the environmental performance of its suppliers and shall keep a record of all findings and any remedial action or improvements in processes or procedures that can be made to reduce any negative environmental impact. Such records shall be provided to Addleshaw Goddard on request.

6.6 Each Supplier shall identify and make know to us, a senior manager within their organisation who shall have overall responsibility for the supplier's environmental performance.

6.7 Suppliers must have an effective internal environmental management program, with adequately trained staff, responsible for environmental impact control and collating and communicating data on key environmental indicators.

6.8 Suppliers shall be in possession of ISO 14001 accreditation or demonstrably working towards ISO 14001 accreditation throughout the contracting period with AG.

## 7 Authority to Commit Expenditure and Payment Process

7.1 Irrespective of the interactions that suppliers may have with many different personnel from Addleshaw Goddard, the ability to commit expenditure with suppliers is strictly controlled. Only certain individuals within AG are authorised to commit AG to expenditure, please contact the Central Procurement Team (centralprocurement@addleshawgoddard.com) for confirmation of such individuals.

7.2 Suppliers must obtain a Purchase Order (PO) number prior to supplying any goods or services to AG, as any invoice without a valid PO number will not be digitally recognised by AG's Purchase to Pay system, and cannot be approved for payment. PO numbers are provided in the PO Report, issued to suppliers via email.

7.3 Any information provided via personal email, faxes and/or telephone call will not create a commitment from Addleshaw Goddard to authorise spend with a supplier. Any supplier who acts upon requests from AG personnel that have not been properly authorised or which do not have a PO number may not be paid for those good or services by Addleshaw Goddard and do so at their own risk.

7.4 Suppliers are responsible for ensuring an accurate and valid invoice, which must quote the correct Purchase Order, is submitted to AG via the Chrome River Purchase to Pay system at the following email address: addleshawgoddard.com-vision@invoice.eu1.chromeriver.com. Statements and queries should continue to be sent to the usual email address: _accountspayable@addleshawgoddard.com. Invoices must not be password protected, and must be addressed to the correct AG Company, as detailed on the PO Report. All invoices will be paid in line with agreed invoice and payment terms. Any incorrectly submitted invoices may be returned to suppliers for correction and resubmission.

## 8 Terms & Conditions for the Purchase of Goods / Services

8.1 AG's Terms and Conditions for the Purchase of Goods and/or Services are attached at 0 (Short-form Terms)

8.2 The Short-form Terms are standard and for use with low value / low risk purchase. These Short-form Terms will only apply to UK contracts where expressly incorporated by reference.

## 9 Data Protection and Information Security

9.1 Suppliers shall comply with all relevant law pertaining to data protection and shall not do or omit to do anything which would cause Addleshaw Goddard to be in breach of such relevant law.

9.2 To the extent that the supplier will be processing personal data on behalf of Addleshaw Goddard, it will do so only in accordance with the terms set out in Appendix 2.

9.3 To the extent that the Supplier will be collecting personal data in respect of which we will be a controller or joint controller with the supplier, the supplier agrees to provide each individual to whom the personal data relates with a Processing Notice.

9.4 Supplier will comply, to the extent relevant to its business and the provision of the services, with the information security requirements set out in Appendix 3.

## 10 Health & Safety Code of Conduct

10.1 Addleshaw Goddard acknowledges and accepts our responsibilities under relevant law for securing and maintaining high standards of health, safety and welfare for all who are directly employed or contracted to work on our Sites.

10.2 Addleshaw Goddard requires that a safe and healthy workplace is provided for all supplier personnel and that of the Health and Safety at Work Act 1974 and all other relevant law pertaining to health and safety is complied with at all times.

10.3 Health and Safety in the workplace shall be the responsibility of a senior member of the supplier's management.

10.4 A copy of AG's general instructions which, together with the specific Site rules, set out the management procedures and requirements to which each supplier will comply, with can be found in 4 below.

## DEFINITIONS AND INTERPRETATION

In this Procurement Policy & Supplier Code of Conduct, the following words shall have the following meanings:

**Addleshaw Goddard**, **AG**, **we** or **our** means any one or more of the entities comprising

**AG LLP** being Addleshaw Goddard LLP a limited liability partnership registered in England and Wales (No. OC 318149) whose registered office is at Milton Gate, 60 Chiswell Street, London EC1Y 4AJ

**AG Service Company Limited** (registered in England with number 07299444) and having its registered office at Milton Gate 60 Chiswell Street London EC1Y 4AG and

(a) any other entity owned or controlled by AG LLP

(b) contract means any contract entered into between the Supplier and Addleshaw Goddard

**Disability Confident Scheme** means the Government scheme designed to encourage employers to recruit and retain disabled people and those with health conditions and includes any variation, replacement or amendment of the same

**DP Law** means relevant law applicable to data protection, the processing of personal data and privacy in force anywhere in the world from time to time including GDPR and the Data Protection Act 2018

**GDPR** means the General Data Protection Regulations ((EU) 2016/679) and Controller, Processor, Data Subject, Personal Data, process/processing/processed, Personal Data Breach, Data Protection Officer take the meaning given to each of these terms in the GDPR

**Processing Notice** means information required to be provided to a Data Subject where Personal Data has been collected from or obtained in respect of such Data Subject, as set out in Articles 13 and 14 of the GDPR or any similar requirement under DP Law

**relevant law** means, in any jurisdiction in which AG or the Supplier provides services, applicable: (a) common law; (b) case law; (c) legislation, enactment, statute, statutory instrument, regulation, by-law; ordinance or subordinate legislation; and (d) binding statutory, industry or other professional regulations, rules, codes, guidance, regulations, practice directions, instruments and provisions

**Services** means the services provided under the Contract

**Supplier** or **supplier** means the person supplying, or wishing to supply, goods or services to AG

The words, **includes**, **including**, **for example**, **such as**, **in particular** and similar phrases do not limit the generality of any preceding words and any words which follow them shall not be construed as being limited in scope to the same class as preceding words where a wider construction is possible

# Appendix 1

Please note there will be some circumstances were we will not consider our general terms and conditions to be suitable. If we are already in discussions with you regarding alternative terms or already have terms in place then Supplier may disregard this 0.

**Terms and Conditions for the Purchase of Goods and/or Services**

**1 Definitions**

1.1 **AG Group** means AG LLP and (a) any entity owned or controlled by AG LLP or any of its members; and (b) any entity owned or controlled by an entity in part (a) or this definition

1.2 **AG LLP** means Addleshaw Goddard LLP a limited liability partnership registered in England and Wales (No. OC 318149) whose registered office is at Milton Gate, 60 Chiswell Street, London EC1Y 4AJ

1.3 **Conditions** means these terms and conditions of purchase for goods and/or services

1.4 **Contract** means the contract between AG and the Supplier for the sale and purchase of the Goods and/or the provision and receipt of the Services

1.5 **Goods** means the goods (if any) described in the Order, or any instalment or part of them to be supplied by the Supplier pursuant to the Contract and shall include any parts used or installed in the performance of the Services

1.6 **Intellectual Property Rights** means all intellectual property rights pertaining to and subsisting in (without limitation) any copyrights, patents, utility models, trade marks, service marks, design rights (whether registered or unregistered), database rights, know-how, technical information, confidential process information, trade and business names (including internet domain names and email address names), proprietary information rights and all other similar proprietary rights as may exist anywhere in the world and all applications for the registration of the same or rights to apply for registration of any of the foregoing

1.7 **AG** means AG Service Company Limited, a company registered in England and Wales (No. 7299444) whose registered office is at Milton Gate, 60 Chiswell Street, London, EC1Y 4AG or such other AG Group entity as has entered into the Contract with the Supplier

1.8 **Order** means the order placed by AG incorporating these Conditions for the supply of the Goods and/or the performance of the Services

1.9 **PO Number** means the purchase order number(s) allocated to each Order and issued to the Supplier

1.10 **Relevant Law** means any statutory requirement; the common law; any binding court decision; and the requirements of any regulator or other industry body to which AG or the Supplier is subject, applicable at the time the Goods are manufactured and sold and/or the Services are provided

1.11 **Services** means the services (if any) described in the Order to be undertaken by the Supplier pursuant to the Contract

1.12 **Supplier** means the person, firm or company to whom the Order is addressed

1.13 **Specifications** means the technical or other requirements (if any) for the Goods or the Services contained or referred to in the Order

**2 General**

2.1 These Conditions shall apply to the Contract to the exclusion of any other terms and conditions contained or referred to in any acknowledgment of order, form of contract, letter or other communication sent by the Supplier to AG.

2.2 No reliance has been placed on any oral or written representations or undertakings except as expressly incorporated. The Contract contains the entire understanding between AG and the Supplier of the subject matter contained herein and supersedes all previous agreements save where AG and the Supplier have entered into a master supply agreement pursuant to which the Order is being raised, in which case, unless expressly stated otherwise, these Conditions shall not apply.

2.3 Any concession made or latitude allowed by AG to the Supplier shall not affect the strict rights of AG under the Contract.

2.4 If in any particular case any of these Conditions shall be held to be invalid or shall not apply to the Contract the other Conditions shall continue in full force and effect.

2.5 No variation to these Conditions or the Contract shall be binding unless expressly agreed in writing by AG and signed on its behalf.

2.6 The Supplier shall not without AG's prior written consent assign, transfer or sub-contract the Contract or any of its rights or obligations thereunder to any other person, firm or company. AG shall have the right to assign, transfer or sub-contract any or all of its rights or obligations under the Contract to any other person, firm or company.

2.7 AG and the Supplier are independent suppliers and this Contract does not create a joint venture nor appoint either party as the agent, employee or partner of the other nor shall either party have any right to bind the other.

2.8 The Contract does not create any rights for third parties.

2.9 Unless expressly stated otherwise: use of the word "including" shall mean "including without limitation"; any list of requirements shall be non-exhaustive; reference to a clause shall mean a clause of these Conditions.

3 Supply of Goods and/or provision of Services

3.1 The Supplier shall supply the Goods and/or provide the Services in accordance with the terms of the Contract and AG's reasonable requirements from time to time.

3.2 The Supplier shall, immediately upon becoming aware, notify AG of any actual or anticipated unavailability of the Goods or Services.

3.3 If the Goods are to be delivered or the Services are to be performed by instalments the Contract shall be treated as a single Contract and not severable.

3.4 Where required by AG, the Supplier shall provide regular statements of Goods delivered, Services performed and invoices raised during the period of time since the last statement.

**4 Quantity, quality, description and standards of performance**

4.1 Without prejudice to any other rights AG may have the Supplier warrants to AG that:

(a) the Goods will:

(i) conform as to quantity, quality and description with the particulars stated in the Contract;

(ii) (without prejudice to clause 4.1(a)(i) above) be of merchantable quality and fit for the purpose held out by the Supplier or made known to it either expressly or by implication by AG;

(iii) be equal in all respects to any samples approved by AG and to the Specifications;

(iv) be capable of any standard of performance specified in the Contract;

(v) comply with all Relevant Law.

(b) the Services will be performed:

(i) in accordance with the Contract and AG's policies and procedures and reasonable requests from time to time;

(ii) by appropriately qualified, trained, skilled and experienced personnel;

(iii) properly and with all due skill, care and diligence;

(iv) in an efficient, professional and workmanlike manner and to the highest standard of quality prevailing in the industry at the time of performance;

(v) in accordance with all Relevant Law.

4.2 The time of delivery of the Goods and of performance of the Services shall be of the essence of the Contract.

**5 Delivery of Goods, Passing of Property, Storage and Rejection**

5.1 The Goods shall be delivered at the time specified in the Order and unless expressly stated otherwise shall take place during AG's normal business hours. The Supplier shall supply AG in good time with any information required to enable AG to accept delivery of the Goods.

5.2 The Goods shall be properly packed and secured in such a manner as to reach their destination in good condition having regard to the nature of the Goods and the other circumstances of the case. AG shall have no obligation to pay for or return packing cases whether or not re-usable.

5.3 All Goods whether delivered to AG's premises or such other premises as are detailed in the Order, shall be accompanied by a detailed advice note stating the Order number and giving full particulars of the Goods supplied.

5.4 Title to the Goods and risk of damage to or loss of the Goods shall pass to AG on delivery to AG in accordance with the Contract.

5.5 AG shall not be deemed to have accepted any Goods until AG has had a reasonable time to inspect them

following delivery, or if later, within a reasonable time after any latent defect in the Goods has become apparent.

5.6 Without prejudice to any other of its rights AG may, by notice in writing to the Supplier, reject any or all of the Goods if the Supplier fails to comply with any of his obligations under the Contract, specifying in the notice the reason for such rejection and requiring the Supplier to remove and, at AG's option, replace or refund the Goods.

5.7 Without prejudice to any other remedies of AG, the Supplier shall forthwith upon a request by AG so to do replace or (at AG's option) repair all Goods which are or become defective during the period of 12 months from the date of delivery where such defect occurs under proper usage and is due to faulty design, or inadequate or faulty materials or workmanship, the Supplier's erroneous instructions as to use, erroneous data or any breach by the Supplier of any provision of the Contract. Repairs and replacements shall themselves be subject to the foregoing obligations for a period of 12 months from the date of delivery, reinstallation or passing of tests (if any) whichever is appropriate after repair or replacement

**6 Performance of Services and use of equipment**

6.1 The Supplier shall perform the Services in compliance with all Relevant Law and such AG policies and procedures as are notified to the Supplier from time to time including polices on health and safety, security, anti-corruption and AG client requirements. The Supplier shall, for the purpose of monitoring compliance with the Contract, permit AG and/or any appropriate regulator access to its premises and full access to all records (in whatever format) relating to the Services.

6.2 The Services shall be performed by the Supplier at the location and at the time or within the period specified in the Order and performed in the manner specified in the Order.

6.3 The Supplier shall ensure any equipment used in the performance of the Services is complete, in first class working order and capable of fulfilling its intended purpose safely and efficiently.

6.4 All equipment made available by AG to the Supplier for the execution of the Contract including any equipment in respect of which the Supplier is performing the Services (Equipment) shall be maintained in good condition by the Supplier and the Supplier shall fully indemnify AG against all loss thereof or damage thereto whilst the same are in the Supplier's possession or control.

6.5 The Equipment shall only be used for the purpose of performing the Services and shall remain AG's property at all times. The Supplier shall have no right to place any lien on any piece of the Equipment. The Supplier shall ensure than any person operating such Equipment is competent and adequately trained to do so.

6.6 The provider shall return any Equipment to AG immediately upon being requested to do so.

6.7 Without prejudice to any other remedies of AG, the Supplier shall forthwith upon a request by AG so to do re-perform any Services found to have been performed defectively within 12 months of the date of their performance.

**7 Charges, Invoicing and Payment Terms**

7.1 The price payable by AG for delivery of the Goods or performance of the Services shall be fixed at the price agreed between the parties in the Contract and unless AG agrees otherwise in writing AG shall not be liable to pay any increase in price or any additional sums.

7.2 The price agreed shall, unless expressly stated otherwise, be net of value added tax (VAT) which AG shall pay to the Supplier in addition to the price at the prevailing rate on receipt of a valid VAT invoice.

7.3 The Supplier shall issue an accurate and valid invoice for the price of the Goods and/or Services in accordance with the Contract or, where no express provision is detailed, shall send an electronic invoice, monthly in arrears, clearly referencing the Contract and relevant PO Number, to: addleshawgoddard.com-vision@invoice.eu1.chromeriver.com . Any statements or queries should be sent to the usual address: _accountspayable@addleshawgoddard.com Invoices will be deemed accurate and valid when it has been approved for payment and entered on to the payment system.

7.4 AG shall make payment to trade Suppliers for Goods or Services (excluding any disputed amounts) within 30 days of the date on which an accurate and valid VAT invoice for the Goods or Services is received by AG, unless otherwise agreed in writing.

7.5 Where AG disputes the whole or any part of an invoice it shall (without prejudice to any other rights) pay all undisputed amounts and AG and the Supplier shall endeavour to settle, as soon as possible, any disputed items. Any overpayments shall be repaid to AG forthwith.

**8 AG's information, data and intellectual property**

8.1 All information supplied by AG to the Supplier in connection with the Contract (Information) is strictly confidential and the Supplier and its officers, employees, agents and subcontractors shall not at any time disclose the Information to any third party without AG's prior written consent.

8.2 The Supplier shall not, without AG's prior written consent, use the name or logo of AG or Addleshaw

Goddard LLP or any entity owned or controlled by AG or Addleshaw Goddard LLP in any public statement.

8.3 The Information shall only be used for the purpose of manufacturing and supplying the Goods to or performing the Services for AG. At AG's request, the Supplier shall promptly return the Information to AG.

8.4 Where the Supplier is requested to process personal data, as defined in the General Data Protection Regulations ((EU) 2016/679) (GDPR), the Supplier shall process such data only in accordance with AG's instructions and as minimum, will comply with the obligations laid out in GDPR Article 28.3.

8.5 The Supplier shall ensure that it and its officers, employees, agents and subcontractors shall comply with all Relevant Law pertaining to privacy, confidentiality and the protection of Personal Data or corporate data (DP Laws).

8.6 The Supplier acknowledges that all Personal Data and any other information covered by DP Laws is confidential Information for the purposes of clause 8.1.

8.7 The Supplier shall comply with and shall ensure that its officers, employees, agents and sub-contractors shall comply with any AG requirement regarding Personal Data including its use, disclosure, non-disclosure, processing and transfer.

8.8 Where the Goods or Services are designed, created or otherwise developed by the Supplier for AG pursuant to the Contract, then all Intellectual Property Rights therein or relating thereto shall belong to AG or a third party nominated by AG absolutely. The Supplier hereby assigns such Intellectual Property Rights to AG or AG's third party nominee as requested by AG with the intent that upon the making or creation thereof the Intellectual Property Rights shall automatically vest in AG or AG's third party nominee.

8.9 The Supplier irrevocably undertakes that neither it nor any other person will assert against AG or any third party any moral rights in or relating to the Intellectual Property Rights referenced in clause 8.8 and warrants that all such moral rights are irrevocably waived and extinguished. For the purpose of this clause 7 "moral rights" shall have the meaning ascribed thereto by the Copyright, Designs and Patents 1988 Act (or any statutory amendment or re-enactment thereof) and all rights similar or corresponding thereto subsisting in any other country of the world from time to time.

**9 Termination and Cancellation**

9.1 AG may, without prejudice to its other rights or remedies hereunder forthwith terminate the Contract by notice in writing to the Supplier:

(a) if the Supplier commits a breach of any of its obligations hereunder and where such breach is remediable does not remedy such breach within 10 working days of the date of written notice from AG of the breach requiring remedy;

(b) if the Supplier, being an individual, (or when the Supplier is a firm, any partner in that firm) shall at any time become apparently insolvent, or shall have a receiving order or administration order made against him or shall make any composition or arrangement with or for the benefit of his creditors or if the Supplier, being a company, shall pass a resolution or the court shall make an order that the company shall be wound up (not being a member's winding up for the purpose of reconstruction or amalgamation) or if a receiver, administrative receiver or administrator shall be appointed of the whole or any part of its assets.

9.2 AG may, without prejudice to its other rights or remedies hereunder forthwith cancel the whole or part of any Order in the event of a failure by the Supplier to ensure delivery of the Goods or performance of the Services within the period of time agreed pursuant to the Contract.

9.3 AG may, without prejudice to its other rights or remedies hereunder, cancel the whole or part of any Order on giving the Supplier not less than 1 calendar month's notice in writing and shall, subject to the receipt of a valid invoice, pay the Supplier for all Goods delivered or Services performed in accordance with the Contract up to the date of cancellation.

9.4 On termination, cancellation or expiry of the Contract or any part thereof, AG shall have the right to enter the Supplier's premises for the sole purpose of removing any Information, Goods, Equipment or other items which are AG's property or which are the property of a third party on whose behalf AG is acting.

9.5 The termination, cancellation or expiry of the Contract or any part thereof shall not affect the continued operation of those provisions which are expressed to survive such termination, cancellation or expiry or to operate or have effect thereafter.

**10 Indemnity**

10.1 The Supplier shall indemnify AG against any and all liability, actions, suits, claims, demands, costs, charges, damages, losses and expenses suffered or incurred by AG and/or for which it may be liable to any third party due to, arising from or in connection with:

(a) the unauthorised acts or omissions, negligence, wilful default or breach of duty of the Supplier, its servants, agents or suppliers in supplying, delivering or installing the Goods or performing the Services;

(b) the breach of any provision of the Contract by the Supplier;

(c) any defect in the workmanship, materials or design of the Goods or their packaging or in the performance of the Services; and

(d) any infringement or alleged infringement of any Intellectual Property Rights for or relating to the Goods or the Services unless such infringement has occurred directly as a result of any Specifications supplied by AG.

10.2 Without prejudice to clause 10.1, AG may without prejudice to its other rights and remedies hereunder claim from the Supplier and the Supplier shall be liable to pay any loss of revenue, profit or other sum arising out of any delay in delivery of Goods or performance of the Services.

**11 Notices**

11.1 Any notice to be served by either party hereunder shall be sent by pre-paid recorded signed-for delivery to the other at the address stated in the Contract and shall be deemed to have been received by the other on the date it is signed for.

**12 Law of the Contract and Jurisdiction**

12.1 The Contract and any non-contractual obligations shall be governed by and construed in accordance with English law and shall be deemed to have been made in England. The parties agree to submit to the non-exclusive jurisdiction of the courts of England. The parties agree that the Contract may be enforced in any court of competent jurisdiction.

# Appendix 2

## Data Protection

**1 Definitions**

1.1 Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under the Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of the Contract, including any Personal Data Breach.

1.2 Data Protection Impact Assessment: an assessment by AG of the impact of the envisaged Processing on the protection of Personal Data.

1.3 Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the DP Law to access their Personal Data.

1.4 Personal Data Record means the record setting out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of data Subjects.

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

1.6 Sub-processor means any third party appointed to process Personal Data on behalf of the Supplier related to the Contract

**2 Data Protection**

2.1 The Parties acknowledge that the Supplier will be processing Personal Data on behalf of AG in connection with the Services. The only processing that the Supplier is authorised to do is detailed in the Personal Data Record and may not be determined by the Supplier.

2.2 The Supplier shall notify AG immediately if it considers that any of AG's instructions infringe DP Law.

2.3 The Supplier shall provide all reasonable assistance to AG in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of AG, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of the Personal Data to be processed.

2.4 The Supplier shall, in relation to any Personal Data processed in connection with its obligations under the Contract:

(a) process such Personal Data only in accordance with this Appendix 2, unless the Supplier is required to do otherwise by Relevant Law. If it is so required the Supplier shall promptly notify AG before processing the Personal Data, unless notification is prohibited by Relevant Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by AG as appropriate to protect against a Data Loss Event, having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that:

(i) Supplier personnel do not process Personal Data except in accordance with the Contract (and in particular this Appendix 2);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Supplier personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Supplier's duties under this paragraph 2.4;

(B) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

(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 AG or as otherwise permitted by the Contract; and

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

(d) not transfer Personal Data outside of the EU unless the prior written consent of AG has been obtained and the following conditions are fulfilled:

(i) AG or the Supplier has provided appropriate safeguards in relation to the transfer (in accordance with GDPR Article 46) as determined by AG;

(ii) the Data Subject has enforceable rights and effective legal remedies;

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

(iv) the Supplier complies with any reasonable instructions notified to it in advance by AG with respect to the processing of the Personal Data;

(e) at the written direction of AG, delete or return Personal Data (and any copies of it) to AG on termination of the Contract unless the Supplier is required by Relevant Law to retain the Personal Data.

2.5 Subject to paragraph 2.6, the Supplier shall notify AG immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under DP Law;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under the Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Relevant Law; or

(f) becomes aware of a Data Loss Event.

2.6 The Supplier's obligation to notify under clause paragraph 2.5 shall include the provision of further information to AG in phases, as details become available.

2.7 Taking into account the nature of the processing, the Supplier shall provide AG with full assistance in relation to either Party's obligations under DP Law and any complaint, communication or request made under paragraph 2.5 (and insofar as possible within the timescales reasonably required by AG) including by promptly providing:

(a) AG with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by AG to enable AG to comply with a Data Subject Access Request within the relevant timescales set out in the DP Law;

(c) AG, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by AG following any Data Loss Event;

(e) assistance as requested by AG with respect to any request from the Information Commissioner's Office, or any consultation by AG with the Information Commissioner's Office.

2.8 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Appendix 2.

2.9 The Supplier shall allow for audits of its Data Processing activity by AG or AG's designated auditor.

2.10 The Supplier shall designate a Data Protection Officer if required by the DP Law.

2.11 Before allowing any Sub-processor to process any Personal Data related to the Contract, the Supplier must:

(a) notify AG in writing of the intended Sub-processor and processing;

(b) obtain the written consent of AG;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Appendix 2 such that they apply to the Sub-processor; and

(d) provide AG with such information regarding the Sub-processor as AG may reasonably require.

2.12 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

2.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. AG may, on not less than 30 Working Days' notice to the Supplier, amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

# Appendix 3

## Information Security: Minimum Requirements

In this Appendix 3, bracketed reference letters/numbers after a requirement relate to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire" or an ISO 27001:2013 Annex A control and references to the following capitalised terms have the following meanings:

**AG** means AG Service Company Limited, a company registered in England and Wales (No. 7299444) whose registered office is at Milton Gate, 60 Chiswell Street, London, EC1Y 4AG

**AG Data** means all data disclosed or made available by AG or a member of the AG Group to the Supplier (including Confidential Information and Personal Data) and all materials to be created or created and data to be generated or generated by the Supplier pursuant to the Contract.

**AG Group** means AG LLP and (a) any entity owned or controlled by AG LLP including AG; and (b) any entity owned or controlled by an entity captured under part (a) of this definition

**AG IT System** means the hardware and software comprising the IT infrastructure which handles all electronic data necessary for the business of the members of the AG Group

**AG LLP** means Addleshaw Goddard LLP a limited liability partnership registered in England and Wales (No. OC 18149) whose registered office is at Milton Gate, 60 Chiswell Street, London EC1Y 4AJ

**Best Industry Practice** means all relevant practices and professional standards relating to the protection of information resources and the maintenance of the confidentiality, integrity and availability of customer data that would be expected of a well-managed, expert service provider performing services substantially similar to the Services to customers of the same nature and size as AG Group

**Client** means any customer, prospective customer or former customer of AG Group

**Cloud** is defined by NIST as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (NIST SP 800-145)

**Confidential Information** means

(a) in the case of AG, any and all information whether recorded or not (and, if recorded in whatever media and by whosoever recorded) disclosed or made available by AG to the Supplier that is by its nature confidential and/or the other party knows or ought to know is confidential including

(i) details of the existing or proposed business carried on by any member of the AG Group including financial, technical, operational, administrative, contractual (including with clients or suppliers or the existence or details of this Contract), marketing and other information or data

(ii) information relating to any client, potential client or former client of any member of the AG Group including the confidential information of any such client, potential client of former client

(iii) AG Data

(iv) information in respect of which any member of the AG Group owes a duty of confidentiality to a third party

(v) information obtained by Supplier as a result of being present at any of the premises of any member of the AG Group

(vi) information disclosed prior to the date of and in connection with this Contract

(vii) any and all other information which is designated by AG as confidential

(viii) plans, analyses, compilations, studies and other documents (in whatever format) which contain or otherwise reflect or are generated from any of the information described in (i) – (vi) above and

(ix) any copies of any of the above

(b) and in the case of the Supplier all information whether recorded or not (and, if recorded in whatever media and by whosoever recorded) disclosed by the Supplier to AG relating to the Contract and which is identified by the Supplier in writing to AG as being confidential

**GDPR** means the General Data Protection Regulations ((EU) 2016/679)

**Handle** means to store, disclose, transfer, access or process data (and Handled shall be construed accordingly)

**Infrastructure** as a Service (IaaS) is defined by Microsoft as "computing infrastructure, provisioned and managed over the internet". IaaS is normally supplied as virtual servers hosted in the Supplier's (or Sub-contractor's) data centres that can be used for any purpose by the AG Group.

**Personal Data** means any data or information which relates to an individual and which is held by or is under the control of any member of the AG Group as defined in the GDPR

**Physical Facilities** means the physical premises where hardware comprising part of the Technical Solution is located

**Platform** as a Service (PaaS) means a computing environment (including servers, storage and operating system) provided and maintained by the Supplier or Sub-contractor, on which the AG Group can develop, run and manage their own applications

**Processing** means any operation or set of operations which is performed on data - such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

**Relevant Law** means

(a) any legislation, enactment, statute, regulation, by-law; ordinance or subordinate legislation in force from time to time to which any member of the AG Group, the Supplier or any third party connected with the Contract is subject

(b) the common law as applicable to any member of the AG Group, the Supplier or any third party connected with the Contract from time to time

(c) any binding court order, judgment or decree

(d) all applicable statutory, industry or other rules, codes, guidance, regulations, instruments and provisions in force from time to time; and

(e) in the case of the Supplier, requirements notified to the Supplier by AG in writing which are born out of the rules and codes of conduct stipulated by any Regulatory Authority or industry body to which any member of the AG Group is subject from time to time

**Regulatory Authority** means in relation to AG Group, any body (including the Solicitors Regulation Authority, any consumer protection body or the Information Commissioner's Office) which has the responsibility of supervising and/or regulating any member of the AG Group and/or any individual performing a role on behalf of any member of the AG Group

**Serverless** computing means a cloud computing model using servers supported by the Supplier or Sub-contractor but with machine resources dynamically allocated as required by the customer. This option is normally used to deploy code which runs when triggered by an event and can be integrated with other services.

**Software** as a Service (SaaS) is defined by Microsoft as a service which "allows users to connect to and use cloud-based apps over the Internet. Common examples are email, calendaring and office tools". Hardware and software are managed by the Supplier or Sub-contractor and the service is usually purchased on a pay-as-you-go basis.

**Special Categories** of Personal Data means any data or information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation which is held by or is under the control of any member of the AG Group

**Sub-contractor** means any third-party supplier from time to time providing goods and/or services directly or indirectly (via any tier of the Supplier's supply chain) to the Supplier in connection with the delivery of the Services. Any Supplier affiliate providing goods or services in connection with the performance of the Services shall be a third party for the purpose of this definition

**Supplier's information** security policy means the documented policy implemented within the Supplier's business which details the procedures, processes, roles and responsibilities, risk assessment tools and risk management tools which comprise the Supplier's information security arrangements and which enable the Supplier as a minimum to comply with the requirements of this Appendix 3

**Supplier IT System** means the hardware and software comprising the IT infrastructure under the direct control of the Supplier which handles all the electronic data necessary for the business of the Supplier

**Technical Solution** means the description of the hardware (including its location(s)) and the software utilised by the Supplier in the provision of the Services which shall comprise the Physical Facilities, the Supplier IT System and may also comprise hardware and software managed by one or more third parties which accordingly may be outside of the direct control of the Supplier

## 1 Risk management

1.1 The Supplier shall:

(a) protect the confidentiality, integrity and availability of all AG Data and any other information relating to AG which is Handled by the Supplier or any of its Sub-contractors;

(b) ensure that such information is not lost, destroyed (including deletion), altered (including corruption), accessed by unauthorised personnel, transferred, mis-used or (without appropriate authorisation) disclosed while it is in the possession and/or under the control of Supplier or any of its Sub-contractors; and

(c) establish an information security risk assessment which includes:

(i) a risk assessment methodology

(ii) regularly analysing and evaluating the risks, at a minimum annually

(iii) awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure

(iv) compliance with defined retention periods and end-of-life disposal requirements

(v) data classification and protection from unauthorized use, access, loss, destruction, and falsification

(vi) risk acceptance criteria; and

(vii) risk treatment plans.

1.2 The Supplier shall at all times have in place such security arrangements as are necessary:

(a) to comply with the requirements of paragraph 1.1;

(b) for the identification and management of operational security risks; and

(c) to mitigate risks to an acceptable level - based on risk criteria, which shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.

1.3 The Supplier shall at all times Handle AG Data in accordance with

(a) Best Industry Practice;

(b) the requirements of the ISO 27001 Standard or equivalent; and

(c) Relevant regulation and law.

1.4 The Supplier shall have in place and comply with a comprehensive information security policy, which is reviewed annually. The Supplier shall provide AG with an up-to-date copy of its information security policy on request.

1.5 The Supplier shall provide the Services and Handle the AG Data in accordance with the Technical Solution as approved in writing by AG.

1.6 The Supplier shall maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. These shall be regularly updated (e.g. change in impacted scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.

**2 Audit**

2.1 The Supplier shall develop and maintain information security audit plans to meet the requirements of ISO27001. Auditing plans shall include reviewing the effectiveness of the implementation of security controls. All audit activities that involve AG or Client data must be agreed with AG prior to commencement.

2.2 The Supplier shall arrange independent audits of its information security arrangements at least annually to ensure:

(a) conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics; and

(b) that the organisation addresses nonconformities of established policies, standards, procedures, and compliance obligations.

2.3 Wherever risks are identified that can be more effectively managed or require better security controls, the Supplier shall update its information security policy accordingly and implement the changes as soon as reasonably practicable in accordance with paragraph 7 of this Appendix 3.

2.4 The Supplier shall carry out regular data protection impact assessments of its information security arrangements to ensure:

(a) appropriate technical and organisational measures, designed to implement data protection principles, have been implemented; and

(b) the necessary safeguards have been integrated into the processing of personal data in order to meet the requirements of the GDPR and protect the rights of data subjects.

2.5 The Supplier will, at all times and on reasonable notice, allow AG or its nominee access to:

(a) all Physical Facilities where AG Data is stored, processed or handled;

(b) all records of the Supplier or any of its Sub-contractors connected with the Services;

(c) any individual involved in the provision of the Services, or with access to any element of the Technical Solution or who has responsibility pursuant to the Supplier's information security policy; and

(d) the procedures, processes and tools utilised in connection with the Contract or in connection with the Supplier's information security policy

for the purpose of auditing compliance with this Appendix 3 and assessing compliance with the Supplier's information security policy.

2.6 The Supplier shall co-operate fully with any external audit and will provide on request any records or other information connected with the Services and in particular connected with the information security obligations of the Supplier or audit information that is required for investigation of security incidents.

## 3 Implementation and management of information security measures

3.1 The Supplier shall ensure that appropriate roles and responsibilities are clearly defined and recorded in the Supplier's information security policy, appropriately allocated and properly fulfilled by individuals within the Supplier's organisation to ensure that:

(a) the Supplier's security obligations under the Contract, including this Appendix 3, are met;

(b) the Supplier's information security policy is fully and properly implemented;

(c) compliance with the Supplier's security obligations and the Supplier's information security policy are monitored, recorded and enforced;

(d) where information security issues are identified, reporting procedures to senior management are in place and are followed appropriately; and

(e) regular risk assessments are undertaken and the Supplier's information security policy is updated to reflect any improvements in risk management which are identified.

3.2 The Supplier shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing of Personal Data and Special Categories of Personal Data is performed in accordance with GDPR, which may include, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it, updating where necessary.

3.3 The Supplier shall implement data input and output validation to reduce potential for misuse, manual or systematic processing errors and data corruption.

3.4 The Supplier shall ensure that application programmable interfaces (APIs) comply with Relevant Law and contractual requirements, and the Supplier shall create, test and deploy any APIs which are required, in line with industry good practice.

3.5 The Supplier shall establish policies, procedures, and mutually-agreed upon provisions and/or terms to satisfy AG's requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.

## 4 Sub-contractor management

4.1 The Supplier shall ensure that AG Data that is hosted within the Supplier IT System is not released to anyone outside the Supplier's organisation without the prior express written approval of AG.

4.2 The Supplier shall ensure that AG Data is only Handled by Sub-contractors in accordance with the agreed delivery model.

4.3 Where the Supplier wishes AG Data to be Handled by a Sub-contractor other than in accordance with the agreed delivery model, the Supplier shall provide AG with full details in writing of the request, clearly describing the business justification, and requesting a change to the delivery model. Where AG in its sole discretion, agrees to such change, it shall issue the Supplier with prior express written approval - in accordance with the procedure for change management detailed in section 7 of this Appendix 3.

4.4 The Supplier shall ensure that its Sub-contractors shall Handle AG Data in accordance with the Contract, including in particular this Appendix 3, such that the requirements placed on the Sub-contractor shall as a minimum be equal to the obligations of Supplier pursuant to the Contract.

4.5 The Supplier shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.

4.6 The Supplier shall manage Sub-contractors such that information security controls are not reduced by the introduction of Sub-contractor products or services.

4.7 The Supplier shall carry out audits on their Sub-contractors handling AG Data at least annually to ascertain their information security controls are maintained and are in accordance with the requirements of this Appendix 3. These audits shall include:

(a) all partners/third party-providers upon which their supply chain depends.

(b) the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.

**5 Human resources security**

5.1 The Supplier shall document and communicate roles and responsibilities of contractors, employees, and third-party users as they relate to information assets and security.

5.2 The Supplier shall carry out such of the following background and reference checks as are appropriate to the role (and jurisdiction) being filled in the recruiting process of all individuals prior to allowing them access to Physical Facilities, AG Data, or the AG IT System:

(a) proof of identity;

(b) proof of address;

(c) proof of right to work;

(d) work references;

(e) proof of continuous employment history;

(f) criminal records check (equivalent to the Disclosure Scotland Checks);

(g) proof of qualifications;

(h) credit reference check;

(i) financial sanctions check; and

(j) any other check required by Relevant Law.

5.3 The Supplier shall establish a security awareness training program for all the Supplier's contractors, third-party users, and employees and mandate completion of this when appropriate. All individuals with access to organisational data shall receive appropriate awareness training and regular updates in organisational procedures, processes, and policies relating to their professional function relative to the organisation. This shall be on induction and annually thereafter.

5.4 The Supplier shall establish a formal disciplinary or sanction policy to cover violation of security policies and procedures by employees. Such employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.

5.5 The Supplier shall inform all workforce personnel and external business relationships of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to Relevant Law.

5.6 The Supplier shall create, update and maintain a record, for all individuals with access to AG Data, of the following information:

(a) full name;

(b) job role;

(c) start date; and

(d) leaving date.

5.7 The Supplier shall establish policies and procedures to ensure the principle of least privilege is followed, and data is accessible only by the minimum number of people necessary to support the service

5.8 Where access is given to AG Group's IT resources and systems, the Supplier shall ensure that by default access be configured with restrictive permissions.

**6 Physical and environmental security**

6.1 The Supplier shall ensure that adequate security measures are in place at all Physical Facilities to ensure that:

(a) security perimeters (barriers such as walls, card controlled entry gates, or manned reception desks) shall be used to protect areas that contain AG Data and / or information processing facilities used to Handle AG Data;

(b) hardware used to Handle AG Data (e.g. servers; telecommunication cabling) and any other vital equipment or services (e.g. power supplies; security cameras or access devices) are protected from damage, unauthorised access and/or interruption;

(c) access to secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access, such as a proximity or swipe card system;

(d) reports on access to secure areas shall be produced and reviewed quarterly;

(e) Data centres shall be equipped with doors:

(i) which are resistant to fire and forcible entry;

(ii) that automatically close immediately after they have been opened; and

(iii) that set off an audible alarm when they have been kept open beyond a certain brief period of time.

6.2 The Supplier shall employ a CCTV system where appropriate, to monitor certain areas of their sites for the purpose of prevention and detection of crime, safety and good management.

(a) All entrances shall be monitored continuously.

(b) CCTV cameras, camcorders, webcams, and other video cameras used shall be placed so that they do not capture passwords, telephone, credit card numbers, encryption keys, or any other security parameters.

(c) CCTV footage shall be stored and available for thirty days.

6.3 Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises shall be controlled by the Supplier, and, if possible, isolated from information processing facilities to avoid unauthorised access.

(a) All deliveries and loading shall be supervised.

6.4 The Supplier must obtain authorisation prior to relocation or transfer of AG Data, or hardware or software used to handle AG Data, to an offsite premises.

6.5 The Supplier shall have a clear desk policy for papers and removable media and a clear screen policy for IT systems.

6.6 The Supplier shall regularly test the security measures in place at the Physical Facilities to risk assess for any vulnerabilities and to enhance measures where security is shown to be inadequate.

**7 Change management**

7.1 The Supplier shall and shall ensure that their sub-contractors shall adhere to policies and procedures for change management, release, and testing which are at least as rigorous as AG's own change management process.

7.2 The Supplier must ensure that developers supporting the service review new and evolving threats, and ensure the service is improved in line with them.

7.3 If the Supplier wishes to implement a change to the Technical Solution or other operational or organisational change connected with the provision of the Services, it may only do so with prior written consent from AG, unless the change:

(a) does not have a detrimental effect on the provision of the Services or the effectiveness of the security measures in place; or

(b) is critical to the continuance of the Services and/or the security of the AG Data.

7.4 The Supplier may only implement a change to the Technical Solution or other operational or organisational change connected with the provision of the Services where the agreed change control procedure has been followed and, in the circumstance described in paragraph 7.3 of this Appendix 3, AG has, in its sole discretion, given prior written approval to the change.

7.5 The Supplier shall separate Production and non-production environments to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.

7.6 The Supplier shall ensure that AG Data is not replicated or used in non-production environments. Any use of Client data in non-production environments requires explicit, documented approval from all Clients whose data is affected.

7.7 The Supplier shall ensure that it has in place a robust configuration management process for the Supplier IT System and Technical Solution, which shall include:

(a) a comprehensive testing regime and approval process for all changes to hardware or its configuration or to software; and

(b) completion of regular comprehensive reviews of servers, firewalls, routers and monitoring platforms to assess optimal configuration and security.

7.8 The Supplier shall ensure that it has in place a robust development management process for the Supplier IT System and Technical Solution, which shall include:

(a) trace back to a living individual, for the development and testing of new software;

(b) removal of any special access paths prior to moving software into production, including any Trojan horses, trapdoors, back-doors, developer security shortcuts, developer universal privileges, in order to ensure that access may only be obtained via normal secured channels; and

(c) ensuring that diagnostic test hardware and software, such as communications line monitors, are used only by authorised Individual and that access to such hardware and software is rigorously controlled and restricted.

7.9 The Supplier shall ensure that the technical and organisational measures required for compliance with the data protection principles and all applicable requirements of GDPR are integral to the Supplier IT System and the Technical Solution.

7.10 The Supplier shall ensure that AG Data is not used to test, demonstrate or evidence any characteristics of the Services provided by the Supplier or any of its Sub-contractors.

**8 Incident management**

8.1 The Supplier shall establish policies and procedures and supporting business processes and implement technical measures, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.

8.2 The Supplier shall establish mechanisms to monitor and quantify the types, volumes, and costs of information security incidents.

8.3 The Supplier shall report all incidents which impact or could potentially impact the provision of the Services, the security of AG Data or the ability of AG to carry out its business, as soon as reasonably practicable and in any event not less than twenty-four hours of the incident coming to the Supplier's attention.

8.4 The Supplier shall report all security violations in accordance with the escalation processes agreed with AG, including all breaches or potential breaches of AG Data.

**9 Vulnerability management**

9.1 The Supplier shall establish policies and procedures and supporting business processes and implement technical measures, for timely detection of vulnerabilities within applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls.

9.2 The Supplier shall conduct annual independent penetration testing, including vulnerability assessment exercises on the Services and the Technical Solution and allow AG visibility of the findings where required.

9.3 The Supplier shall conduct vulnerability assessments on at least a monthly basis, and shall ensure that security vulnerability assessment tools or services which are implemented can accommodate any virtualisation technologies which might be used (e.g. are virtualisation aware).

9.4 The Supplier shall establish policies and procedures, implement supporting business processes and ensure technical measures to:

(a) prevent the execution of malware on organisationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

(b) prevent the introduction of malicious software (including viruses and spyware) into the Technical Solution and/or into the AG IT System through the provision of the Services;

(c) promptly detect any malicious software and/or viruses attempting to access any element of the Technical Solution and/or into the AG IT System through the provision of the Services;

(d) implement regular updates of anti-malware software tools;

(e) report and escalate as appropriate any malicious software and/or viruses incidents in-line with agreed and documented AG incident management procedures; and

(f) ensure that incidents are immediately notified to AG if there is an actual or suspected Virus in:

(i) The AG IT System;

(ii) any part of Technical Solution to which the AG IT System interfaces; or

(iii) anything to be delivered by the Supplier or any sub-contractor to AG as part of the provision of the Services.

**10 Network security management**

10.1 The Supplier shall implement all appropriate security measures to protect the AG Data within the Supplier IT System and at all interfaces where AG Data enters or leaves the AG IT System or any third party electronic environment (Network).

10.2 The Supplier shall carry out regular tests to check the security of the Network and make such changes as are necessary to remove any actual or suspected security weaknesses.

10.3 The Supplier shall document a data flow map for AG Data which depicts accurately and comprehensively how AG Data flows and is stored across the AG IT System, the Supplier IT System and any Network or other permitted external destinations.

10.4 Where the Supplier uses APIs, supplier shall ensure that such APIs shall be open and published to ensure support for interoperability between components and to facilitate migrating applications.

10.5 The Supplier shall provide a report to AG on all security weaknesses identified and on any remedial action taken.

10.6 The Supplier shall establish policies and procedures and supporting business processes and implement technical measures, for the use of encryption protocols for protection of data in storage (e.g., file servers, databases, and end-

user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) in accordance with Relevant Law, including:

(a) the Supplier shall encrypt AG Data in transit and at rest;

(b) the Supplier shall apply encryption to all non-console administrative access and web-based management, using industry recognised technologies such as Virtual Private Network (VPN), Secure Sockets Layer (SSL) or Transport Layer Security (TLS);

(c) the Supplier shall protect all AG Data transmitted over third party public networks with strong encryption techniques of at least 256 bits, such as Secure Sockets Layer (SSL), or Internet Protocol Security (IPsec); and

(d) where the Supplier manages cryptographic keys, the Supplier shall ensure that these have identifiable owners (binding keys to identities) and that effective key management policies are established.

10.7 Where the Supplier delivers a service using Cloud infrastructure or services Supplier shall:

(a) hold a Cloud Policy which sets out the management and governance of cloud platforms;

(b) ensure that multi-factor authentication is in place for externally hosted cloud platforms;

(c) ensure that Cryptography is deployed within the cloud environment, using AES-256 block cipher algorithm and encryption of traffic and data applying TLS Cipher Suite (TLS 1.2 and higher). Key management process to be implemented and maintained;

(d) be aware of the cloud services used to provide services to the Firm which can be requested by the Firm in inventory form in line with due diligence requirements;

(e) instruct vulnerability scanning and penetration testing of the cloud environment and vulnerabilities found shall be mitigated and prioritised depending on criticality;

(f) harden virtual machines within the cloud to maximise security;

(g) monitor the cloud environment to ensure performance, unauthorised access, tampering and data integrity;

(h) ensure that management of virtualisation platforms is restricted to AG Group's IT staff and service provider staff;

(i) ensure that if templates are used in the deployment of virtual resources they are reviewed at least annually for suitability and security issues;

(j) inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks, and inform AG of any changes to provision of such services;

(k) ensure that AG data is appropriately segmented in a multi-tenant environment from any other tenant users, based on the following considerations:

(i) established policies and procedures;

(ii) identity and access control mechanisms;

(iii) isolation of data, and sessions that mandate stronger internal controls and high levels of assurance; and

(iv) compliance with Relevant Law;

(l) ensure that Network environments and virtual instances are designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed by the Supplier at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls; and

(m) use secure (e.g., non-clear text and authenticated) standardised network protocols for the import and export of data and to manage the service, and shall make available a document to AG detailing the controls involved.

**11 Access control**

11.1 The Supplier shall ensure that all access to the Technical Solution and AG Data is:

(a) strictly controlled - physically and logically, and that user access is audited on at least an annual basis;

(b) restricted to authorised Individuals only as per defined segregation of duties to address business risks associated with a user-role conflict of interest.;

(c) granted only when an Individual inputs authorised identity authentication information; and

(d) revoked as soon as no longer required or when the relevant individual is no longer engaged by the Supplier or assigned to the Services.

11.2 The Supplier shall establish procedures to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access.

11.3 The Supplier shall maintain, protect and retain user access logs as a high priority, so that all obligations under Relevant Law can be met and potentially suspicious network behaviours, file integrity anomalies and security breaches can be investigated.

11.4 The Supplier shall ensure that Passwords for the Supplier's IT Systems:

(a) are technically enforced;

(b) are at least nine characters;

(c) are different from their associated unique identifier;

(d) contain characters from at least three or more of the following:

(i) numbers;

(ii) upper-case letters;

(iii) lower-case letters;

(iv) symbols (e.g. &^%);

(e) are subject to change on first login, if provided by an administrator;

(f) are subject to change every 90 days;

(g) cannot be changed by the user more than once per day;

(h) are different from the previous 24 passwords; and

(i) are supported by multi-factor authentication for all remote access and administrator access to AG Data.

11.5 The Supplier shall ensure that individual accounts on the Supplier IT System must be locked out after four invalid logon attempts.

**12 Access logs and record keeping**

12.1 The Supplier shall implement the following audit procedures:

(a) audit logging;

(b) monitoring; and

(c) alerting

to ensure that any action which takes place in the Technical Solution or which is effected by an individual or other person is logged and can be proven to have taken place.

**13 Business continuity and disaster recovery**

13.1 The Supplier shall back-up all AG Data in accordance with agreed service levels, to ensure security of the AG Data and the uninterrupted provision of the Services.

13.2 The Supplier shall implement and maintain appropriate and adequate business continuity arrangements that comply with:

(a) Best Industry Standards; and

(b) ISO22301 or equivalent

that detail agreed Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Incident response plans shall involve impacted clients and other critical business relationships.

13.3 The Supplier shall:

(a) test the business continuity measures on a regular basis and in any event not less than annually or upon significant organisational or environmental changes;

(b) record the test results; and

(c) make the test results available to AG upon request.

13.4 The Supplier shall develop and implement adequate disaster recovery arrangements that;

(a) ensure the agreed RTOs and RPOs can be achieved; and

(b) take account of the AG critical functions and processes supported by the Services; and

(c) take account of all interdependencies within the Technical Solution, both internal, within the Supplier IT System and external between the Supplier IT System and any third party electronic environment.

13.5 The Supplier shall:

(a) test the disaster recovery arrangements on a regular basis and in any event not less than annually;

(b) record the test results; and

(c) make the test results available to AG on request.

13.6 The Supplier shall ensure that availability, quality, and adequate capacity and resources are planned, prepared, and measured to deliver the required system performance in accordance with Relevant Law. The Supplier shall make projections of future capacity requirements to mitigate the risk of system overload.

**14 Asset management**

14.1 The Supplier shall ensure it has a clear complete understanding and a written record of the type of AG Data being Handled as part of the Services. Supplier shall keep a comprehensive record of the names of the AG IT Systems being used in the provision of the Services.

14.2 The Supplier shall classify and handle the AG Data in accordance with requirements set out by AG, including:

(a) establishing policies and procedures for the labelling, handling, and security of data and objects which contain data; and

(b) implementing mechanisms for label inheritance for objects that act as aggregate containers for data.

14.3 The Supplier shall ensure that, when no longer needed for bona fide business purposes, or as required by Relevant Law or pursuant to contractual obligations, or as requested by AG, AG Data within the Supplier IT System or otherwise in its possession or under its control (which shall include being under the control of Sub-contractors pursuant to the Technical Solution):

(a) that is stored electronically, is securely and permanently deleted/erased and/or destroyed so that such AG Data is not recoverable; and

(b) which comprises hardcopy materials, are cross-cut shredded, incinerated, or pulped.

14.4 The Supplier shall provide to AG, five (5) business days in advance of the termination or expiry of the Contract, a copy of all AG Data at no cost to AG. All structured and unstructured data shall be available to AG in an industry-standard format (e.g. doc, xls, pdf, logs, and flat files).

14.5 The Supplier shall, within five (5) business days of providing AG with a copy of all AG Data pursuant to paragraph 14.4 of this Appendix 3, dispose of all AG Data in accordance with paragraph 14.3 of this Appendix 3.

14.6 The Supplier shall establish policies and procedures with supporting business processes and implement technical measures for the secure disposal and complete removal of AG's data from all storage media, ensuring data is not recoverable by any computer forensic means.

14.7 The Supplier shall, upon request by AG, provide evidence acceptable to AG that AG Data has been permanently and securely destroyed in compliance with paragraph 14.3 of this Appendix 3.

# Appendix 4

## Health & Safety Information

### General Site Rules – AG Sites

In this Appendix 4, the following terms have the following meanings:

**AG** means AG Service Company Limited, a company registered in England and Wales (No. 7299444) whose registered office is at Milton Gate, 60 Chiswell Street, London, EC1Y 4AG

**AG Group** means AG LLP and (a) any entity owned or controlled by AG LLP which is notified to the Supplier from time to time, including AG; and (b) any entity owned or controlled by an entity notified to the Supplier under part (a) of this definition

**AG LLP** means Addleshaw Goddard LLP a limited liability partnership registered in England and Wales (No. OC 18149) whose registered office is at Milton Gate, 60 Chiswell Street, London EC1Y 4AJ

**Premises** means such premises from which members of the AG Group operate from time to time

**Site** means, for each address which comprise the Premises, all areas of the building occupied by AG, (or where detailed, it's tenants), at such address including all public and restricted access areas together with all outdoor areas of the address and the areas immediately surrounding the address including access roads, pavements and delivery bays

**Sub-Contractor** means any third party supplier from time to time providing goods and/or services directly or indirectly (via any tier of the Supplier's supply chain) to the Supplier in connection with the performance of the Services. Any Supplier Affiliate providing goods or services in connection with the performance of the Services shall be a third party for the purpose of this definition

**Works** means a specific piece of inspection, testing, maintenance or repair work

**Works Permit** means written consent for specific Works to be carried out

**1 Introduction**

1.1 AG acknowledges and accepts its statutory responsibilities for securing and maintaining high standards of health, safety and welfare for all who are directly employed or contracted to work on the Site.

1.2 AG require all Suppliers who work in areas for which they have direct responsibility to comply with the requirements of the Health and Safety at Work Act 1974 and all other relevant statutory provisions.

1.3 A copy of this instruction will be handed to all Suppliers who are engaged to carry out work on the Site.

1.4 These general instructions, together with the specific Site rules, set out the management procedures and requirements, which each Supplier will comply with.

1.5 Suppliers are responsible for controlling the work of any Sub-Contractors which they employ. This will include providing AG with safety documentation confirming the competence of Sub-Contractors, i.e. evidence of competence, specific risk assessments and method statements.

**2 Before Commencement of Works**

2.1 No Supplier will be permitted to commence Works without giving AG at least 48 hours' notice except in an emergency situation or ongoing routine maintenance.

2.2 No Supplier will be allowed to commence work without:

(a) The Supplier informing AG of any risks likely to be posed by any plant, equipment or materials to be used during the Works, prior to bringing them onto the Site.

(b) The Supplier ensuring that all plant, equipment, materials and systems of work used during the contract comply with the Health and Safety at Work Act and all other statutory requirements.

(c) All areas of operation, access and storage etc. having been clearly defined and agreed with the person engaging them.

2.3 In the case of Suppliers who have been engaged by AG to carry out work in areas for which the AG has direct responsibility, the Supplier must in addition:

(a) Provide a written statement of the Supplier's Health and Safety Code of Conduct;

(b) Provide a written statement as to the safety precautions to be taken to protect their employees and other persons on the Site from their work activities;

(c) Provide evidence of insurance cover to indemnify AG in respect of any negligence resulting in personal injury and/or death, or damage to property and/or plant arising out of or in connection with the contract work;

(d) Provide written COSHH assessments and Hazard Data Sheets for all substances to be used on the Site; and

all such information will have been sought and obtained prior to the Supplier carrying out the work in question.

**3 During the Works**

3.1 Each AG approved Supplier must:

(a) provide a list of all personnel who will work on Site;

(b) provide details of the supervisor/safety co-ordinator appointed by them to liaise on all relevant health and safety matters.

3.2 Each Supplier shall be responsible for ensuring that, at the start and completion of each shift, they and/or their employees complete the 'Permit to Access' form provided.

3.3 Each Supplier will be responsible for ensuring that all their employees are aware of their individual responsibilities under the Health and Safety at Work etc. Act 1974 and these rules.

3.4 The Supplier is not permitted to use any tools (hand or powered), plant, ladders or equipment belonging to AG.

3.5 The Supplier is prohibited from using any of the Site services such as electricity, gas, steam or compressed air without specific authorisation.

3.6 The Supplier shall ensure that there is effective control of dust generated by the Works.

3.7 The Supplier will ensure that noise is kept to a minimum throughout the Works.

3.8 The Supplier will take any steps necessary to control the risk of exposure of his employees or other persons to asbestos fibres. If asbestos is suspected or discovered, the Supplier must stop work immediately and notify the relevant AG contact. On no account must the work continue. The area must be secured to prevent any persons entering it and all work equipment and clothing must remain in the affected area.

3.9 The relevant AG contact will then take appropriate steps to ensure the risks from the asbestos are minimised and the asbestos is dealt with in accordance with AG procedures.

3.10 Suppliers must avoid using substances which are likely to emit fumes or odours. Where it is not practical to avoid using substances, i.e. there is no less hazardous substitute, then they must ensure that all air conditioning units, ventilation equipment, windows and other means where by fumes may enter the building, have been closed, isolated, turned off or otherwise protected.

3.11 Where Suppliers are carrying out chlorination work in relation to the water systems, or other similar treatment involving flushing or purging of a system, then they must ensure that the drainage run being utilised is free from any blockages.

3.12 Where Suppliers are working alone they must make arrangements for the work area to be checked regularly or a procedure in place to alert a second person that a problem may have occurred. This could include ringing / reporting to a nominated person at set intervals. This procedure must be agreed with AG before work commences.

## 4 Work Permits

4.1 The Works Permit system shall be managed by the Supplier for any Works carried out by itself or any Sub-Contractors

4.2 The following high risk types of work cannot be carried out in any area under the control of AG without a Works Permit:

(a) All roof work;

(b) All work on atria, cupolas, canopies and other such high level glass or fragile structures;

(c) All excavations and excavation work;

(d) All demolition work;

(e) All confined spaces;

(f) All work on pressure systems;

(g) The use of all cartridge tools;

(h) All hot work (including the use of asphalt and bitumen boilers);

(i) All welding and flame cutting;

(j) All work on live electrical systems or systems above 240v where workers are exposed to live conductor;

(k) All cranes, hoists, and tower access equipment (but not goods lifts and passenger lifts);

(l) All overhead work which includes the use of scaffolding, tower scaffolding and mobile elevating platforms;

(m) The use of flammable and highly flammable liquids (except for cleaning and decorating materials); and

(n) Where it is shown by risk assessment that a Works Permit is necessary for:

(i) work where there is a high risk of injury (such as exists in working with or near live electricity) or where it is not sufficient to rely upon either human behaviour or systems of work;

(ii) all usually straightforward operations which may interact with others to cause a serious hazard;

(iii) all maintenance work which can only be carried out if normal control measures are removed;

(iv) all work which itself produces new significant hazards; and

(v) areas of lone working that carry a potential of injury – e.g. lift examination / repairs in the shaft, other work at height.

4.3 The issue of a Works Permit will depend on the knowledge and experience of the Supplier, the contents of risk assessments and method statements provided, other work activities in the vicinity and weather conditions.

4.4 A Works Permit will not be issued on behalf of AG until and unless the Supplier is satisfied that all necessary measures to make safe and specific conditions are in place.

## 5 Fire Precautions

5.1 The Supplier shall ensure all personnel are trained in the fire and emergency procedures which apply to the Site, including ensuring that Supplier personnel:

(a) are familiar with the fire warning signal and means of activating it;

(b) are aware of the location of firefighting equipment and report any use of such equipment;

(c) comply with smoking controls on the Site;

(d) are instructed not to misuse, remove or interfere with fire-fighting equipment; and

(e) do not obstruct means of escape.

5.2 The Supplier shall:

(a) advise AG of any flammable mixtures, liquefied petroleum gases or explosive substances to be used or stored on the Site;

(b) not discharge fuel anywhere on the Site;

(c) obtain a Works Permit prior to commencing any operations involving the use of any flame or heat producing equipment; and

(d) provide additional fire-fighting equipment as appropriate.

**6 Electricity**

6.1 The Supplier will not be permitted to use the Site electricity supply without the agreement of AG

6.2 The Supplier will ensure that:

(a) all practicable precautions are taken to prevent danger to any person from any live electrical cable or apparatus or any electrically charged overhead cable or apparatus;

(b) all electrical connections to the Site supply are only carried out by a qualified electrician;

(c) all installations and appliances are without avoidable safety risk and conform to the "Electricity At Work Regulations 1989" and all associated statutory provisions and accepted practices, including current IEE wiring regulations;

(d) it provides suitable switching/isolating at the tool or equipment end of any extension cable used;

(e) all electrical equipment and temporary installations are disconnected or isolated before leaving the area of work or at the end of each working session;

(f) all portable tools are of maximum voltage 110v, supplied from a transformer;

(g) all portable tools and electrical appliances, including extension leads and multi-socket connectors, in use at the premises are examined and tested regularly, are fit for safe operation;

(h) electrical equipment and appliances will be visually examined prior to each use to check for obvious faults such as loose wires or damaged plugs, and to remove damaged items from Site and that documentation is available to confirm this; and

(i) no personnel work on any high tension electrical equipment unless in possession of a valid Works Permit.

**7 Access Equipment**

7.1 The Supplier will be responsible for providing all access equipment necessary to enable the contract work to be carried out, they will ensure that all equipment is:

(a) in a safe and serviceable condition.; and

(b) is used in accordance with statutory requirements, all relevant Health and Safety Executive Guidance and manufacturer's instructions.

**8 Security**

8.1 The Supplier will:

(a) permit the searching of any one of their employees, vehicles or property at any time either on the Site or within the immediate vicinity;

(b) report any use of, damage to, or removal from Site;

(c) isolate and secure all plant, equipment and vehicles when not in use and before leaving the Site;

(d) not store any explosive, flammable or noxious substances on Site, even temporarily, without permission;

(e) report any losses of property immediately the loss is discovered; and

(f) not take photographs or copy documents belonging to AG without permission.

**9 Accidents**

9.1 The Supplier will ensure that all accidents are immediately reported to AG.

**10 Completion of Works**

10.1 On completion of all Works the Supplier will:

(a) reinstate and make good/decorate any surface as necessary to the complete satisfaction of AG;

(b) remove all refuse, surplus materials and debris from the Site; and

(c) make arrangements for final inspection and 'signing off'' of Works with the AG representative. Inspection shall be completed at the discretion of the AG representative.

## DISCLAIMER:

These instructions and rules are not intended to supersede any specific legal requirements or Health and Safety Executive recommendations. If any conflict is identified, it should be raised with AG's Representative.

# DOCUMENT CONTROL

| | | | |
|---|---|---|---|
| **STATUS:** | Live | **EFFECTIVE DATE** | November 2023 |
| **NEXT REVIEW DATE:** | November 2024 | **FRAMEWORK:** | Practice Manual |
| **REFERENCE NUMBER:** | 77922538v1 | **APPROVED BY:** | Michael Chisnall |
| **OWNER:** | Procurement | **AUTHOR:** | Lizzie Tinkler |

# VERSIONS / REVISIONS

| REVISION DATE | VERSION (IMANAGE NO.) | SUMMARY OF CHANGES | UPDATED BY |
|---|---|---|---|
| September 2018 | 10/6920988/6 | Original | Rosemary Cummings |
| Sept 2019 | 10/6920988/7 | Supplier management to include ongoing DD Goods in the supply chain to be traded fairly | Rosemary Cummings |
| June 2020 | 7.1 (draft) | Added cloud controls to Appendix 3 | Matt Rhodes |
| July 2020 | 7.2 (draft) | Updated after feedback from MCMAK | Matt Rhodes |
| 15th July 2020 | 7.3 (draft) | Updated after feedback from RFC | Matt Rhodes |
| August 2020 | 10/6920988/8 | Formatting; interpretation; consistent use of definitions; Supplier positive obligations | Rosemary Cummings |
| February 2021 | 6920988/11 | Formatting; structural changes and additional wording in policy and code of conduct introductions; amendments to PO & invoice terminology | Lizzie Tinkler |
| October 2021 | 6920988/12 | Version control error corrected; invoice email address corrected; additional wording RE: exit / BC / DR plans added to supplier requirements | Lizzie Tinkler |

| | | | |
|---|---|---|---|
| October 2022 | 6920988/13 | Version 13 - InfoSec amends + Diversity and Inclusion update + typo's rectified. | Lizzie Tinkler |
| November 2023 | 77922538v1 | Annual review. Additional controls covering cloud security. | Michael Chisnall |

addleshawgoddard.com

Aberdeen, Doha, Dubai, Edinburgh, Glasgow, Hamburg, Hong Kong,
Leeds, London, Manchester, Muscat, Singapore and Tokyo*

*a formal alliance with Hashidate Law Office