INFORMATION SECURITY AND RISK MANAGEMENT POLICY

1. **DEFINITIONS**

1.1 The following terms shall have the meanings ascribed to them.

Cloud Services	means computing infrastructure, platforms, systems, or software which are provided and managed by the Supplier, or by a third party provider ("Cloud Services Provider") acting in conjunction with the Supplier, in order to provide computing services via the internet
Company Materials	means Company Confidential Information, Company Data, and Company Personal Data
Company's Systems Environment	means all the Group Companies' information systems (including hardware, software, any equipment, or communications devices) which are accessible to the Supplier in connection with this Agreement
CSO	means a party's Chief Security Officer (or their authorised representative). In the case of the Company this shall be the Group Chief Security Officer
Cyber Essentials	means the scheme introduced by the UK Government to provide cybersecurity assurance certification, which is operated by the UK National Cyber Security Centre (NCSC) and for which IASME provides certification services, and which includes: (a) Cyber Essentials (CE), a self-assessment scheme; and (b) Cyber Essentials Plus (CE+), an audited self-assessment scheme www.gov.uk/cyber-essentials-scheme-overview
Data Breach (relevant breach)	means a breach by the Permitted Supplier of Industry Rules or Data Protection Laws and Regulations, which has been directly caused by a breach by the Supplier of its obligations under this Agreement
Facility or **Facilities**	means any kind of building intended to house any Company Materials, Supplier Personnel, or the Supplier's Systems Environment used in connection with the Supplier's obligations under this Agreement
Good Security Practice	means: (i) established and approved under the Supplier's system of corporate governance, and (ii) designed, implemented, operated, maintained, monitored, reviewed, and improved from time to time, all in accordance with Good Industry Practice and in

	compliance with the technical and organisational measures and practices that are required by ISO 27001; and generally accepted Information Security standards, practices, techniques, methods, and guidelines published by recognised authorities and organisations regarding Information Security which the Supplier would reasonably be expected to align to in accordance with Good Industry Practice, including ISO, NIST, SANS, OWASP, CIS, and which are relevant to the Supplier's obligations under this Agreement
each of **ISO 27001, ISO 27701, ISO 27005, ISO 27017, ISO 27018** and **ISO 27035**	means, individually, the international standard for Information Security management as published by the International Standards Organization and as updated from time to time and which are: (a) BS EN ISO/IEC 27001 "Information Security Management System (ISMS) requirements"; (b) BS EN ISO/IEC 27701 "Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines"; (c) BS EN ISO/IEC 27017 "Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services"; (d) BS EN ISO/IEC 27018 "Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"; (e) ISO/IEC 27005 "Information technology. Security techniques. Information security risk management"; and (f) ISO 27035 shall mean and include: (i) BS ISO/IEC 27035-1:2016 "Information technology. Security techniques. Information security incident management - Principles of incident management"; (ii) BS ISO/IEC 27035-2:2016 "Information technology. Security techniques. Information security incident management - Guidelines to plan and prepare for incident response"; and (iii) BS ISO/IEC 27035-3 "Information technology. Information security incident management - Guidelines for ICT incident response operations"
IASME	means the IASME Consortium Ltd (company number 07897132) and which is the sole body authorised by the NCSC to provide certification to the Cyber Essentials scheme. iasme.co.uk

IEC 62443	is a set of security standards that are dedicated and/or applicable to asset owners, operators, and suppliers of OT to safeguard industrial automation and control systems. Understanding IEC 62443
ICS	Industrial Control Systems are defined as programmable systems or devices that interact with the physical environment.
Information Risk	means any physical or logical risk that might adversely affect Information Security of the Company's Systems Environment, the Supplier's Systems Environment, or any Goods and/or Services provided by (or on behalf of) the Supplier under this Agreement
Information Security	means: (a) to protect and preserve: (i) the physical and logical confidentiality, integrity, and availability of Company Materials the Company's Systems Environment (to the extent that the Supplier's activities may impact such environment), and the Supplier's Systems Environment, including to prevent any unauthorised access to, or disclosure, theft, loss, damage, destruction, or misuse of, the foregoing; and (ii) related properties of information such as authenticity, accountability, and non-repudiation; (b) to detect, prevent or otherwise manage, and report, any Information Risk; (c) to detect, prevent, manage, and report any Security Defect, Information Security Incident, or Information Security Breach; and (e) compliance with all Laws and Data Protection Laws and Regulations applicable to the transmission, storage, and processing (including physical and logical security) of information and information systems
Information Security Breach	shall mean any circumstances, Incident or event where the Supplier or the Company knows of, or reasonably suspects, an event which compromises Information Security, or physical security, and which adversely affects or may reasonably be expected to adversely affect the Company, Company Materials, the Company's Systems Environment, the Supplier's Systems Environment, the Facilities, or any Goods and/or Services provided by (or on behalf of) the Supplier under this Agreement.
Information Security Incident	means a single or a series of unwanted or unexpected physical or logical events affecting the Supplier's System Environment or the Company's Systems Environment, or any Goods and/or Services

	provided by (or on behalf of) the Supplier under this Agreement and which constitutes: (i) a failure of information security governance, policy, standards; (ii) a failure of procedures, processes, technologies or other controls; or (iii) a previously unknown condition that may be security relevant (any of which has a significant possibility of compromising business operations or threatening Information Security) or indicates that any of the foregoing may have occurred
Information Security Management System or **ISMS**	means the governance, policies, standards, procedures, processes, and technologies instituted by the Supplier in accordance with Good Security Practice to provide Information Security
Information Security Manager	means the person appointed by the Supplier with the requisite experience and expertise to ensure that the Supplier complies with the provisions of this Policy
Malicious Software	means any software program or code intended to (i) destroy, steal, damage, impair, corrupt or otherwise disrupt the intended operation of computer networks, computer systems, Software or data
OT	Operational Technology (same as ICS) are defined as programmable systems or devices that interact with the physical environment.
PCI Cardholder Data	means any or all: (i) any cardholder data pertaining to any payment card, including: the full primary account number, cardholder name, expiration date, service code, or (ii) any security-related information including: card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, or PIN blocks, or as otherwise defined by PCI SSC
PCI CDE	means the environment, including the people, processes, and technology, which are used to collect, store, process, or transmit PCI Cardholder Data
PCI DSS	means the Payment Card Industry Data Security Standard as published and updated from time to time by the PCI Security Standards Council www.pcisecuritystandards.org Compliance with PCI DSS is an obligation for any entity which may collect, process, store or transmit PCI Cardholder Data, or facilitate any of the same, whether or not as part of a payment card transaction

PCI QSA	means a Qualified Security Assessor qualified in accordance with the procedures and requirements set forth by PCI SSC
PCI Security Standards Council or **PCI SSC**	means the body established to develop and drive adoption of data security standards and resources for safe card payments worldwide. https://www.pcisecuritystandards.org
Policy	means this Information Security and Risk Management Policy
Security Defect	means (i) any Malicious Software, or (ii) any defect of, misconfiguration of, vulnerability in, or unauthorised change to, any Software or the Supplier's Systems Environment
Security Incident Management Plan	means the policy, standards, plans, procedures, and operations which are established in accordance with ISO 27001 and/or ISO 27035 (or a standard which is substantially equivalent) to identify, record, manage, resolve and report any Information Security Incident or Information Security Breach
Software	means any software program or code (including operating system, software application, software solution, patch, program file, firmware, application software macro, or application programming interface (API)), whether standalone, a component of a larger program, solution, or system, or otherwise dependent on another program, solution, or system, regardless of their intent or purpose and which is, or can be made to be, executable
Supplier's Systems Environment	means, without limitation, all information systems (including hardware, software, equipment, communication devices, or any Cloud Services) owned or controlled by or on behalf of the Supplier (and any Subcontractors of the Supplier) which are or may be used in connection with the provision of Goods and/or Services under this Agreement.

1.2 Capitalised terms used in this Policy, and which are not defined herein shall have the meanings ascribed to them elsewhere in this Agreement.

1.3 Any obligation not to do anything shall include an obligation not to suffer, permit or cause that thing to be done.

2. GENERAL PROVISIONS

2.1 This Policy sets out the Supplier's obligations regarding Information Security in connection with the performance of its obligations under this Agreement.

2.2 Notwithstanding anything to the contrary elsewhere in the Agreement, in the event of any inconsistency or divergence between the information security obligations set out in this Policy and any lower standards required of the Supplier elsewhere in the Agreement, the obligations set out in this Policy shall prevail.

2.3 The Supplier shall ensure that the Supplier's Systems Environment and the Supplier's Facilities are adequately and appropriately secured to avoid or minimise the occurrence of any Information Risk.

2.4 The Supplier shall, and shall procure that its Subcontractors shall, ensure that the Supplier's Systems Environment, the Goods and/or Services, and any Software, used or provided pursuant to or in consequence of the Supplier's obligations under this Agreement, shall be free from any Security Defect.

2.5 The Supplier shall provide to the Company on request, written evidence, and assurance in respect of the security of any Company Materials processed by the Supplier as may be reasonably required by the Company to comply with its obligations under applicable Laws.

2.6 The Supplier shall, on an ongoing basis, assess and properly manage Information Risks in all matters relating to the Services and shall, therefore, continuously improve its ISMS and the Information Security of the Supplier's Systems Environment and any Goods and/or Services provided by (or on behalf of) the Supplier under this Agreement.

3. INFORMATION SECURITY MANAGEMENT

3.1 The Supplier shall:

3.1.1 appoint an Information Security Manager who shall be responsible for ensuring the Supplier's compliance with all security requirements set out in this Policy;

3.1.2 ensure a suitable replacement deputises for the Information Security Manager when said individual is unavailable for any reason; and

3.1.3 inform the Company of the individual appointed as the Information Security Manager, and the individual appointed to deputise for the same, prior to the commencement of the delivery of the Goods and/or Services, and as such appointments are made from time to time.

4. INFORMATION SECURITY COMPLIANCE AND ASSURANCE

4.1 **Compliance**: Notwithstanding the security standard the Supplier has adopted, it shall ensure that it conforms with the requirements of ISO 27001 and where the Supplier utilises any Cloud Services, those of ISO 27017, and where the Supplier processes personal data in any Cloud Service, those of ISO 27018.

4.2 The Supplier shall institute an ISMS which meets the requirements of Good Security Practice and shall ensure that the requirements of this Policy, (or their substantial equivalent), form an integral part of its ISMS. Such ISMS shall conform to ISO 27001 and the Supplier shall:

4.2.1 create and maintain a scope statement (which includes all the Goods and/or Services provided under this Agreement);

4.2.2 at least annually perform, and record the results of, a risk assessment (to be conducted in accordance with ISO 27005 or its substantial equivalent) which shall include any Information Risks relevant to the provision of the Services ("**Risk Assessment**");

4.2.3 create and maintain a plan, to track to remediation all Information Risk identified by any Risk Assessment ("**Risk Treatment Plan**");

4.2.4 create and maintain a record of all Information Risks, corresponding Risk Treatment Plan, the status of such Information Risks, (including whether

unmitigated, accepted, or treated), the controls to mitigate such risks, and the status and effectiveness of such controls ("**Risk Register**"); and

4.2.5 create and maintain a Security Incident Management Plan.

4.3 **Independent assurance**:

4.3.1 The Supplier shall obtain and shall maintain for the duration of its obligations under this Agreement (or parts thereof), certification of its ISMS to ISO 27001 by a nationally accredited certifying body.

4.3.2 The Supplier shall provide to the Company on request formal evidence of such certification including an unredacted copy of any associated Statement of Applicability (SoA) in accordance with the requirements of ISO 27001.

4.3.3 In addition to its obligations under paragraph 4.3.1, if the Goods and/or Services are enabled by, or provided in conjunction with, Cloud Services: (i) the Supplier shall obtain, and shall for the duration of its obligations under this Agreement shall ensure that such Cloud Services shall be certified by a nationally accredited certifying body to ISO 27017, (ii) if Personal Data is transmitted, stored, or otherwise processed then the Cloud Services shall be certified by a nationally accredited certifying body to ISO 27018, and (iii) the Supplier shall ensure that the Cloud Services form an integral part of its ISMS.

4.3.4 The Supplier shall provide to the Company on request formal evidence of such certification of any such Cloud Services, including an unredacted copy of any associated Statement of Applicability (SoA), in accordance with the requirements of ISO 27001 and, as applicable, ISO 27017 and/or ISO 27018.

5. INFORMATION PROCESSING & HANDLING

5.1 Without prejudice to the Supplier's obligations in respect of data protection and/or confidentiality elsewhere in this Agreement, the Supplier shall:

5.1.1 ensure that Company Materials are not compromised, lost, destroyed, or corrupted in any way;

5.1.2 ensure that it only uses and retains those Company Materials necessary to perform its obligations under this Agreement; and

5.1.3 ensure that only those Supplier Personnel who need to have access to Company Materials for the purposes of performing the Supplier's obligations under this Agreement shall be granted access.

5.2 The Supplier shall not, and shall procure that its Subcontractors shall not, copy, disclose, transmit, store, or otherwise process in any manner any Company Materials nor make available the same to any third party, without the Company's prior agreement in writing (unless expressly required by law).

5.3 The Supplier shall ensure that appropriate and adequate technical and organisational measures are in place to protect any Company Materials when printed or otherwise obtained in physical format (from or on behalf of the Company) by Supplier Personnel. All such physical Company Materials shall be stored in a secure locked container whenever left unattended irrespective of whether such physical Company Materials may be at risk of unauthorised access.

5.4 The Supplier shall, and shall procure that its Subcontractors shall:

5.4.1 not store or process Company Materials in, or access Company Materials from, on any service accessible to, and intended for, the public including DropBox, Facebook, Gmail etc.; and

5.4.2 not permit.

(i) any unauthorised third party or Supplier Personnel; or

(ii) any unauthorised computer, network, or Software,

any physical or logical access to (including any ability to view or record) Company Materials, whether from within the Supplier's Systems Environment or by any form of remote access to it.

6. ACCESS TO THE COMPANY'S SYSTEMS ENVIRONMENT

6.1 This section (ACCESS TO THE COMPANY'S SYSTEMS ENVIRONMENT) shall only be applicable if the Supplier has any physical or logical connection to any systems, software, or networks of any Group Company.

6.2 The Company shall not grant access to the Company's Systems Environment by any form of physical or logical connection without prior agreement in writing from the Company's CSO. Such agreement shall be contingent on the Supplier providing the Company with detailed designs of such access for review and approval by the Company. If the Company grants its approval, the Supplier shall ensure that it only accesses the Company's Systems Environment in the manner set out in the detailed designs.

6.3 Where the Supplier is granted access to the Company's Systems Environment for the purposes stated in this Agreement, the Supplier shall not access or use the Company's Systems Environment other than to the extent strictly necessary for the purpose of fulfilling its obligations under this Agreement.

6.4 The Supplier shall keep authentication credentials (including passwords, certificates, tokens, and biometric data) that enable access to the Company's Systems Environment strictly confidential and shall only disclose the same to any third party, or to Supplier Personnel, who are authorised by the Supplier in writing for the purposes of this Agreement, unless specifically authorised to do so by the Company in writing.

6.5 The Supplier shall comply with any controls and limitation of access specified by the Company in writing in relation to access to the Company's Systems Environment. Such limitations may include defining access to specific systems and times and dates of access as applicable.

6.6 The Company shall, during the term of this Agreement, provide advice to the Supplier as is reasonably required to overcome any problems that the Supplier may have in accessing or operating the Company's Systems Environment. As such the Supplier must not attempt to resolve any problems, which, as a result, could jeopardise the Company's Systems Environment. Any problems encountered in the use of the Company's Systems Environment must be reported immediately to the Company through the agreed channels relevant to this Agreement.

6.7 To the extent that Supplier Personnel use any part of the Company's Systems Environment the Supplier shall, and shall procure that Supplier Personnel shall, always comply with the Company's Acceptable Use Policy when performing the Services under this Agreement. For avoidance of doubt the Supplier agrees that it shall be responsible for making itself aware of the prevailing version of the Company's Acceptable Use Policy.

7. SUPPLIER'S SYSTEMS ENVIRONMENT

7.1 The Supplier shall be responsible for the provision, implementation, change management, support and maintenance of the development, configuration, management, and policies for the Information Security of any hardware or Software within the Supplier's Systems Environment including any form of remote access by any individual, computer, or Software, which the Supplier permits.

7.2 Where, pursuant to or in consequence of providing the Services and/or Goods or otherwise performing its obligations under this Agreement, the Supplier provides physical or logical access to the Supplier's Systems Environment and which facilitates or otherwise enables any access to Company Materials, the Company's Systems Environment, and the Goods and/or Services, including any connections intended to provide remote access or remote working ("**Remote Access**"), the Supplier shall:

7.2.1 not grant access to any third party or Supplier Personnel, except those required for the performance of its obligations under this Agreement;

7.2.2 ensure that any third party or Supplier Personnel granted such access or use shall comply with the Supplier's ISMS and the provisions of this Policy;

7.2.3 ensure that such access or use is monitored, controlled, and limited to that necessary for the purpose of performing its obligations under this Agreement; and

7.2.4 ensure that authentication credentials (including passwords, certificates, tokens, or biometric data) that enable any access to the Supplier's Systems Environment shall be kept strictly confidential and shall not be provided to any third party or Supplier Personnel unless required for the provision of the Services and shall not be provided without the Supplier's prior authorisation in writing.

7.3 If the Supplier provides connection to the Supplier's Systems Environment for any third party, Supplier Personnel, computer, or Software, by means of any form of Remote Access it shall:

7.3.1 consider and treat all such Remote Access as an integral part of the Supplier's Systems Environment and subject to the requirements of this Policy;

7.3.2 create and maintain technical and organisational standards to govern and manage Remote Access and integrate these into its ISMS;

7.3.3 not permit any Remote Access without adequate encryption and authentication (e.g. virtual private network);

7.3.4 pursuant to paragraph 15 (Logging and Monitoring) continuously monitor, periodically record the compliance of, and immediately record any non-compliance of, all Remote Access. The Supplier shall keep such records for a minimum of ninety (90) days;

7.3.5 not permit any Remote Access which does not comply with the requirements of this Policy; and

7.3.6 shall immediately discontinue, disconnect and/or prevent any Remote Access which fails to comply with the requirements of this Policy.

8. ENCRYPTION

8.1 The Supplier shall ensure that technical controls (including data encryption, authorisation, authentication) and procedural controls (including policies, user awareness, training) are implemented for all Company Materials wherever such may be stored including all portable devices (including laptops, tablets, notebooks, mobile phones) and removable media (including CDs, DVDs, USB storage devices, backup tapes), databases, servers, and any cloud-based services that contain Company Materials.

8.2 The Supplier shall ensure that Company Materials transferred electronically outside of the Supplier's Systems Environment, or over any public network, are encrypted.

8.3 The Supplier shall select and implement any encryption standard, including any method, technique, protocol, or algorithm (individually and collectively an "**Encryption Algorithm**") used pursuant to paragraphs 8.1 and 8.2 in accordance with Good Security Practice. The Supplier shall ensure that encryption functions provided by office productivity software (including Microsoft Office, Adobe Acrobat, OpenOffice), but excluding online office productivity services (including Office365, Google Docs) and data compression tools such as WinZip (providing that an encryption standard of AES 256 or higher is used), shall not be relied upon to protect Company Materials without the Company's prior agreement in writing.

8.4 The Supplier shall not and shall procure that its Subcontractors shall not implement nor otherwise rely upon any Encryption Algorithm which is, according to Good Security Practice, considered obsolete, or is insecure. For these purposes, an Encryption Algorithm is insecure when, due to inherent weakness within a method or process of the Encryption Algorithm, data encrypted by it can be retrieved by means other than that intended by the Encryption Algorithm. All data encrypted by such an insecure Encryption Algorithm can no longer be protected or secure ("**Data at Risk**").

8.5 The Supplier should not implement nor otherwise rely upon any deprecated Encryption Algorithm. To the extent the Supplier does implement or rely upon any deprecated Encryption Algorithm it shall only do so in accordance with Good Security Practice and provided it implements adequate compensating controls.

8.6 To the extent the Supplier or its Subcontractors implement or otherwise rely upon a deprecated Encryption Algorithm the Supplier shall: (i) record and track, in its risk register, the use of such (by itself or its Subcontractors), and (ii) update or otherwise replace such deprecated Encryption Algorithm at the earliest opportunity.

8.7 In the event that a deprecated, or any other, Encryption Algorithm is implemented, and the Supplier becomes aware that it is obsolete or is insecure the Supplier shall, and shall procure that its Subcontractors shall, without delay (i) inform the Company, (ii) replace all implementations of such insecure Encryption Algorithm, and (iii) re-encrypt all Data At-Risk, all-in accordance with Good Security Practice.

8.8 In the event of Information Security Breach which arises directly or indirectly because of the use of a deprecated or insecure Encryption Algorithm the Supplier shall be liable for such breach.

9. SECURE DISPOSAL OF COMPANY MATERIALS

9.1 The Supplier shall promptly destroy or delete, in accordance with Good Security Practice (including NIST Special Publication 800-88, NCSC guidance or services), Company Materials (including call recordings) when no longer required (wherever and howsoever stored) and (unless otherwise instructed by the Company) on termination or expiry of this Agreement or (if later) on completion of any exit plan which may be required by this Agreement.

9.2 The Supplier shall treat any Company Materials which are no longer needed as confidential waste for the purposes of such destruction.

9.3 If any Company Materials reside on any item of hardware, including media, ("**Hardware**") the Supplier shall destroy such Company Materials pursuant to paragraphs 9.1 and 9.2 prior to the disposal of the Hardware. The Supplier shall provide independent verifiable evidence that all such Hardware has been processed in accordance with Good Security Practice to ensure the data contained on it cannot be subsequently retrieved or restored.

10. INFORMATION SECURITY INCIDENTS AND BREACHES

10.1 The Supplier shall create, operate, maintain, review, improve from time to time, and periodically test (not less frequently than annually) a Security Incident Management Plan.

10.2 The Supplier shall record and manage any Information Security Incident, or Information Security Breach in accordance with requirements of this Policy, and the Supplier's Security Incident Management Plan.

10.3 The Supplier shall promptly notify the Company of the occurrence of any Information Security Breach, and in any event no later than twenty-four (24) hours of becoming aware of the same, such notification to be made: a) by e-mail to privacy@centrica.com and resilience@centrica.com; b) by telephone to the Global Operations Centre on +44 (0)1753 494500; and c) to a Company Representative or other agreed channels relevant to this Agreement.

10.4 The Supplier shall not unreasonably refuse any request by the Company to collaborate in resolving any Information Security Incident or Information Security Breach.

10.5 The Supplier shall investigate any Information Security Incident or Information Security Breach in accordance with Good Security Practice and shall, for any material Information Security Breach, perform a computer forensic investigation and shall provide to the Company any report arising from any investigation, subject always to any contractual obligation of confidentiality which it may owe to a third party.

10.6 The Supplier shall report to the Company, at the earliest opportunity, the facts of any Information Security Breach as they are known to the Supplier and shall, throughout any investigation by the Supplier, provide to the Company regular reports on the progress of any investigation at a frequency and in such detail as shall be agreed between the parties.

10.7 In the event of an Information Security Breach the Supplier shall, without undue delay, provide to the Company upon request any records, reports, computer logs (howsoever and wheresoever stored), documents, or other information required or implied by this Policy, subject always to any contractual obligation of confidentiality the Supplier may owe to a third party.

10.8 Any Information Security Incident or Information Security Breach shall be Confidential Information for the purposes of this Agreement.

11. PCI DSS

11.1 This section (PCI) shall only be applicable if the Supplier performs any payment card transactions, or collects, stores, processes, transmits any Cardholder Data, or facilitates any of the same e.g. by redirecting the browser (of a person seeking to make a card payment) to a payment services processor.

11.2 If, to the extent required by its obligations under this Agreement, the Supplier collects, stores, processes, or transmits PCI Cardholder Data, or facilitates any of the same, for or on behalf of the Company, the Supplier:

11.2.1 warrants and represents that it holds and shall maintain for the duration of this this Agreement a valid PCI DSS Attestation of Compliance (AoC) for each of the payment card services it provides under this Agreement and agrees that each such AoC shall be issued (or if a SAQ AOC, countersigned) by a PCI QSA;

11.2.2 shall restrict the disclosure of PCI Cardholder Data to those of its Supplier Personnel or Subcontractors who are required by it to meet its obligations under this Agreement;

11.2.3 shall always indemnify each Group Company, its officers, employees and agents, and keep such Group Company and its officers, employees and agents indemnified, from and against any Losses incurred or for any fine, levy or sanction imposed on the Group Companies for any non-compliance with PCI DSS by the Supplier, Supplier Personnel and/or Subcontractors; and

11.2.4 acknowledges that it is responsible for the security of PCI Cardholder Data to the extent that the Supplier could impact the security of the PCI CDE relevant to its obligations under this Agreement and shall improve security in respect of PCI Cardholder Data in accordance with Good Security Practice, the requirements of this Policy and as agreed between the parties.

11.3 For the avoidance of doubt the Supplier shall:

11.3.1 only collect, store, process, transmit or facilitate any of the same for, PCI Cardholder Data pursuant to or in consequence of performing the Services; and

11.3.2 interpret in the broadest sense any reference in this paragraph 11 to facilitating the collection, storage, processing, or transmission of PCI Cardholder Data (for example, providing a re-direct of a customer's browser to a payment service provider) and such facilitation shall require a valid AoC pursuant to paragraph 11.2.1.

12. OPERATIONAL TECHNOLOGY (OT)

12.1 This section (OT) shall only be applicable if the Supplier provides Goods and/or Services that are classed as OT. OT or Industrial Control Systems (ICS) are defined as programmable systems or devices that interact with the physical environment. They are typically used to monitor or control industrial processes and can also provide visibility and/or status of those processes to other platforms and systems within the organisation. The Supplier shall comply with the latest industry standards, regulations, and best practice guidance for securing OT. This shall include, but not be limited to the following:

12.1.1 OT risks shall be managed.

Appropriate organisational structures, policies, and processes shall be in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions. The Supplier shall ensure effective governance, risk management processes, asset management and supply chain management are in place for supplied Goods and/or Services.

12.1.2 OT shall be protected against cyber-attack.

Proportionate security measures shall be in place to protect the network and information systems supporting essential functions from cyber-attack. These measures include; service protection policies and processes, identity and access control, data security, system security, resilient networks and systems and staff awareness and training.

12.1.3 Cyber security events shall be detected.

Capabilities shall be implemented to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions. These capabilities include security monitoring and proactive security event discovery to detect anomalous events.

12.1.4 The impact of cyber security incidents shall be minimised.

Capabilities shall be implemented to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary. Effective response and recovery planning shall be implemented with continuous improvement and lessons learned.

12.2 IEC 62443 is a set of security standards that are dedicated and/or applicable to asset owners, operators, and suppliers of OT to safeguard industrial automation and control systems. These standards offer a robust framework, which covers the topics of risk assessment, security policies, network architecture, access control, incident response, and security testing. The Supplier shall conform to the guidance of IEC 62443 when supplying Goods and/or Services that comprise of OT.

13. VULNERABILITY AND PATCH MANAGEMENT

13.1 In this paragraph 13 (Vulnerability and Patch Management), the term "**Software Provider**" shall mean (i) the Supplier's own internal Software development function; and (ii) any third party Software used by the Supplier in the provision of the Goods and/or Services, and any Software used or provided pursuant to or in consequence of the supplier's obligations under this Agreement.

13.2 The Supplier shall, in accordance with Good Security Practice, patch Software in accordance with the Software Provider's instructions, including as follows:

13.2.1 install emergency patches within a period of fourteen (14) days of release by the Software Provider; and

13.2.2 install security or other patches deemed critical by Software Provider within a period of one (1) month, and other patches within a period of three (3) months, of release by the Software Provider.

13.3 The Supplier shall record and report unsuccessful patching against Software Providers' patch releases. In this paragraph 'unsuccessful' patching shall mean that (i) a patch was not installed within the period required; (ii) a patch repeatedly failed to install correctly; or (iii) the Supplier chose not to install a patch pursuant to paragraphs 13.2.1 or 13.2.2.

13.4 Where the Supplier's Systems Environment is connected to the Internet or to other organisations/networks (including the Company's System Environment), the Supplier shall, in order to detect and remediate any and all Security Defects:

13.4.1 regularly (but not less frequently than monthly and on the occurrence of any major change to the Supplier's Systems Environment that may affect the

Information Security of the Supplier's Systems Environment, the Goods and/or Services, or the Company's Systems Environment), perform a vulnerability scan (a "**Scan**") of the Supplier's Systems Environment;

13.4.2 regularly (but not less frequently than annually and on the occurrence of any major change to the Supplier's Systems Environment that may affect the Information Security of the Supplier's Systems Environment, the Goods and/or Services or the Company's Systems Environment) perform a security penetration test (a "**Pen Test**") of the Supplier's Systems Environment;

13.4.3 categorise and record the findings of a Scan or Pen Test using a vulnerability scoring system (e.g. Common Vulnerability Scoring System) to assign a severity level as follows:

(a) Critical Vulnerability

(b) High Vulnerability

(c) Medium Vulnerability

(d) Low Vulnerability

(e) Informational

13.4.4 create, or cause to be created, a report of the findings of each Scan or Pen Test (a "**Test Report**");

13.4.5 remediate (a) critical or high findings within a period of one (1) month; and (b) other findings within a period of three (3) months of the issuance of the relevant Test Report;

13.4.6 within a further period of one (1) month of such remediation, validate for each finding that remediation is effective by performing a subsequent Scan or (for critical, high, or medium findings only) Pen Test and produce a report of the findings of such subsequent Scan or Pen Test (a "**Validation Test Report**");

13.4.7 provide to the Company on request a complete and unredacted copy of such Test Report or Validation Test Report; and

13.4.8 provide to the Company on request a consolidated report which shall track to remediation any vulnerabilities which have been discovered by any Scan or Pen Test.

13.5 The provisions of paragraphs 13.4.7 and 13.4.8 shall be subject always to the Supplier's contractual obligation of confidentiality which it may owe to a third party.

14. SOFTWARE DEVELOPMENT

14.1 To the extent that the Supplier or its Subcontractors develop Software pursuant to or in consequence of performing its obligations under this Agreement, the Supplier shall, and shall procure that its Subcontractors shall, do so in accordance with Good Security Practice.

14.2 If, pursuant to or in consequence of providing Goods and/or Services, or in otherwise performing its obligations under this Agreement, the Supplier performs any Software development, the Supplier shall create, implement, maintain, review, and improve from time-to-time appropriate code development policies, procedures, practices, and test methods and techniques, prior to such development being performed.

14.3 Where any Software developed pursuant to paragraph 14.2 may require installation within the Company's Systems Environment the Supplier shall be responsible to make itself aware

of all relevant Company policies, procedures, and working practices for Software development and shall adhere to the same.

14.4 Without prejudice and subject to any obligation it may have regarding performance or acceptance tests required by this Agreement, the Supplier shall test any and all Software it develops in connection with the Goods and/or Services to ensure such Software contains no Security Defect and the Supplier shall not deploy or deliver such Software prior to the successful completion of such tests.

14.5 The Supplier shall not, either in the development or in the test of any Software to be used in connection with the Goods and/or Services or in otherwise performing its obligations under the Agreement, use any of the Company's production data nor use any data which may cause the Company to become non-compliant with Data Protection Laws and Regulations.

15. LOGGING AND MONITORING

15.1 **Logging**: For investigating and reporting every Security Defect, Information Security Incident or Information Security Breach the Supplier shall, for each security, system, and user event which occurs in each system and application within the Supplier Systems Environment ("**Event**"), (i) protect and preserve the evidence of any such Event, and (ii) create and maintain a record of such Events ("**Log**").

15.2 The Supplier shall ensure that each Log and the Events it records are protected and preserved against any corruption, alteration, or unauthorised destruction and the Supplier shall not authorise the destruction of any Log except in accordance with this Policy.

15.3 The Supplier shall ensure that, apart from any operational requirement to monitor the Events it records, each Log shall be securely stored such that the destruction or unavailability of a system or application, or a Facility housing the same shall not also cause the destruction or unavailability of the corresponding Logs.

15.4 the Supplier shall retain each Log for a minimum of six (6) months, or such longer period as may be specified by the Company in writing.

15.5 The Supplier shall, as far as it is practicable, ensure that each system and application is synchronised to a common precise time reference and that (i) each Event is recorded, and (ii) Log created, using a precise reference to time, which shall be common to all systems and applications, and the Supplier shall protect and preserve this information.

15.6 The Supplier shall ensure that each Log shall, at a minimum, record the following Events, and where (i) 'User' means and includes standard user account, privileged user account, system account, application account, (ii) 'Object' means and includes means and includes file, directory, application, database record, User account, and (iii) each record of the following Events shall include: User identifier, permissions, group memberships, privileges, and other details, where relevant:

15.6.1 User authentication success;

15.6.2 User authentication failure;

15.6.3 User account creation (where user accounts are not managed exclusively by an external system);

15.6.4 User account deletion (where User accounts are not managed exclusively by an external system);

15.6.5 Bulk data export;

15.6.6 Bulk data import;

15.6.7 any Object actions including create, access, change, delete, copy, move;

15.6.8 The precise date and time of each Event; and

15.6.9 An unambiguous title and summary of each Event recorded.

15.7 **Monitoring**: The Supplier shall correlate and monitor Events for indications of any: (i) Security Defect, (ii) Information Security Incident, and (iii) Information Security Breach and shall respond to each in accordance with Good Security Practice, the requirements of this Policy and its own policies, standards, and procedures.

16. PHYSICAL SECURITY

16.1 This section (PHYSICAL SECURITY) shall only be applicable if the Supplier is responsible for the physical security of its own Facilities (including office, data centre, contact/call centre) used in provision of the Goods and/or Services to any Group Company.

16.2 The Supplier shall comply with the physical security requirements set out in ISO 27001 (or its substantial equivalent) and shall create, maintain, review, and update from time to time, appropriate policies, standards, and procedures for physical security which shall apply to its Facilities.

16.3 To the extent that it is responsible for the physical security of Facilities used in connection with the Supplier's obligations under this Agreement the Supplier shall apply the requirements of paragraph 4 in respect of physical security.

16.4 The Supplier shall comply with paragraph 15 (Logging and Monitoring) in respect of any and all physical security events. For these purposes, "Events" shall be construed to include any physical security events and "Logs" shall be construed to include any records made of physical security events whether these are recorded manually or electronically.

17. AWARENESS & TRAINING

17.1 The Supplier shall ensure that all Supplier Personnel complete an information security awareness training programme.

17.2 The information security awareness programme shall:

17.2.1 ensure Supplier Personnel are aware of their obligations in relation to Information Security;

17.2.2 ensure Supplier Personnel are made aware of relevant Supplier ISMS and data processing policies; and

17.2.3 be successfully completed by Supplier Personnel:

(a) within thirty (30) working days of being employed by the Supplier;

(b) before such Supplier Personnel are given access to any of: (i) the Company's Systems Environment, (ii) Company Materials, or (iii) the Services; and

(c) at regular intervals thereafter, such intervals to be no more than twelve months.

17.3 The Supplier shall create, maintain, and regularly review records ("**Records**") of each Supplier Personnel's completion of the information security awareness training programme,

and it shall promptly revoke or deny access to any Supplier Personnel who have not successfully completed the Supplier's information security awareness training programme.

17.4 The Supplier shall ensure that Supplier Personnel shall only be involved in the provision of the Services or parts of the Services for which they have been adequately trained.

18. SUBCONTRACTOR SECURITY MANAGEMENT

18.1 The Supplier shall procure that throughout the Term its Subcontractors shall comply with the requirements of this Policy and it shall:

18.1.1 ensure that any Subcontractor contract includes obligations which are substantially the same as, and in any case no less onerous than, the provisions of this Policy, including independent assurance of the Subcontractor's ISMS which shall be the same as, or substantially equivalent to, that at paragraphs 4.3.1 and 4.3.3;

18.1.2 create, maintain, and improve from time to time, Subcontractor security management policy, standards, and procedures for the purpose of managing and demonstrating compliance with paragraph 18.1.1, in respect of each Subcontractor;

18.1.3 upon request, provide the Company with names and addresses of its Subcontractors together with details of the goods, services and/or Software they provide; and

18.1.4 in accordance with the provisions at paragraph 18.1.2, investigate its Subcontractors compliance with the contractual provisions referred to in paragraph 18.1.1 and provide to the Company on request the details of its findings. The frequency of such investigations shall be established by the Supplier based on a risk assessment of the relevant Subcontractor (which shall be at least once during the term of the contract between the Supplier and the respective Subcontractor), save that the Supplier shall investigate any Subcontractor's compliance with the Policy if reasonably requested to do so by the Company.

19. GOVERNANCE, RECORDS AND REPORTING

19.1 Any matters relating to Information Security and any records or reports required or implied by this Policy shall be provided by the Supplier to the Company as required by this Agreement, or otherwise on request to the Company's CSO.

19.2 The Supplier shall create and maintain for the term of the Agreement a record which shall include details of every non-compliance, of any of the provisions of this Policy ("**Non-Compliance Record**").

19.3 The Supplier shall ensure that:

19.3.1 any non-compliance shall be added to the Non-Compliance Record promptly following its discovery; and

19.3.2 the Non-Compliance Record shall be provided (i) to the Company as required by this Agreement, or (ii) annually to the Company's CSO, and (iii) on request, to the Company's CSO.

AUDIT (The right to audit)

19.4 The right of audit includes a right for the company nominated Auditor to enter any of the Supplier Premises to inspect and take copies of such books and records and to interview members of the Supplier Personnel as is required for the purposes referred to in clause 10.3, although the audit shall be conducted remotely, through video conferencing and screen sharing, wherever possible and where this is appropriate.

19.5 In addition to any other audit requirements elsewhere in the Agreement, the Supplier shall, on request from the Company, permit an Auditor to inspect the Supplier's Systems Environment, and take copies of information including procedures, settings, configuration files, and Logs (i) not more than once in any year in order to provide an Auditor with assurance as to the Supplier's compliance with the information security provisions of this Agreement, or (ii) at any time in order to investigate any actual or reasonably suspected Information Security Breach.

19.6 The Supplier shall perform, and make a report of the findings of, a risk-based security audit of the Supplier's System Environment (i) annually during the term of this Agreement, and (ii) upon any major change to the Supplier's Systems Environment. The Supplier shall provide a copy of such report to the Company on request.

19.7 **Purpose of audit**: The purpose of any audit carried out under this clause 10 shall be to: (a) provide the Company with assurance as to the Supplier's compliance with this Agreement; (b) to enable the Company to investigate any complaints or queries of or provide information required by a Regulatory Authority or any customers of the a Group Company relating to the Services or the conduct of the Supplier, the Supplier Personnel or the Subcontractors; or (c) to investigate any suspicion of fraud or wrongful practice on the part of the Supplier, the Supplier Personnel or the Subcontractors. Notwithstanding the foregoing, audits carried out under clauses 10; will be for the purpose of enabling the Company to carry out its mid-year and end of year financial reporting audits and prepare any related financial statements.

19.8 **13.3 Conduct of audit:** The Supplier shall cooperate with the Auditor and will provide or procure such reasonable access and assistance as the Auditor reasonably requires enabling the Auditor to exercise the rights set out in clause 10 for the purposes in clause 10.3. Except where the audit is undertaken in respect of suspected fraud or breach or by a Regulatory Authority which stipulates that no notice should be given, the Company shall (a) provide at least ten (10) Business Days' written notice of the audit; (b) shall conduct the audit (or procure it is conducted) within normal business hours; and (c) shall use reasonable endeavours to ensure that the conduct of each audit does not disrupt the business of the Supplier or delay the provision of the Services by the supplier.