DATA SECURITY SCHEDULE

INFORMATION SECURITY, PHYSICAL SECURITY & BUSINESS CONTINUITY MANAGEMENT

These terms are supplementary to the Main Terms. All capitalised terms that are not defined in this Appendix shall have the definitions set out in the Main Terms.

Applicable Security Law Requirements	means any applicable requirements arising out of law, statute, byelaw, regulation, order, regulatory policy, guidance or industry code, rule of court or directives relating to information security.
Business Continuity Incident	means any event as a result of which the Business Continuity Plan is invoked.
Business Continuity Management Programme	means a proactive process to identify key operations and recovery requirements from which Business Continuity Plans may be developed.
Business Continuity Plan	means a plan produced by the Supplier invoked upon the occurrence of a Business Continuity Incident which provides step by step guidance around the recovery of services to an agreed recovery point.
Business Impact Analysis	means a process that identifies and evaluates the potential effects of natural and man-made events on business operations.
Company Assets	means the Company personnel, the Company Data or relevant infrastructure.
Company Customer Data	means information relating to the Company's clients and customers (or those of any Group Company).
Company Data	means all data (including but not limited to the Company Customer Data), tables, information, text, drawings, codes, diagrams, images or sounds which are embodied in any electronic or tangible medium, including compilations of any of the foregoing, and which are: (a) processed by, or a product of, the Services; (b) generated by the Supplier or a Supplier Company or a sub-contractor of the Supplier in carrying out the Supplier's obligations under this Agreement; or generated by or on behalf of the Company or a Group Company.
Company Systems	means systems of the Company or a Group Company.
Development Environment	means the environment made available for the creation and development of programs or software products prior to being released into a Testing Environment.
GDPR Regulation	means General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).
Information Commissioner's Office	means ICO is the UK's independent body responsible for upholding information rights and data privacy for individuals.
Information Security Controls	means controls to protect the confidentiality, integrity or availability of data.
Minimum Business Continuity Objective	means the minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during an incident, emergency or disaster.
Personally Identifiable Information (PII)	means information that can be used to identify an individual person e.g. name, date of birth, address.
Physical Security Controls	means controls to prevent unauthorised physical access to Supplier or Supplier company premises.
Physical Security Incident	means any event where there is, or potentially could be, unauthorised access to, or use of, or interface with Company Assets under the Supplier's or a

	Supplier Company's or any of the supplier's (or, as the case may be, a Supplier Company's) sub-contractors' control.
Production Environment	means an environment where the real-time staging of programs that run an organisation are executed, and includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
Public Cloud Services	means any data hosting, processing or storage service which is provided to the Supplier by a Third Party, where the service is provided on infrastructure owned and located at the third party's premises, and the service is made available over the internet using infrastructure shared amongst clients and customers.
Recovery Point Objective	means the point in time to which work needs to be restored following a Business Continuity Incident.
Recovery Time Objective	means the time objective for restoration of Business as Usual in the event of Business Continuity Incident.
Relevant Systems	means systems that host Company Data, either the Company Systems or Supplier Systems.
Security Incident Management Process	means monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events.
SMEs	means Subject Matter Experts.
Supplier Company	means a member of the group of companies of which the primary Supplier is the parent company, or where the supplier company is considered an affiliate of a group of companies.
Supplier Personnel	means any employee, officer, agent or other person whatsoever acting for the Supplier or otherwise under the control and direction of the Supplier, a Supplier Company or of any of the Supplier's Approved Sub-Contractors.
Supplier Network	means technology network or system of computers operated by the supplier or a Supplier Company or any of the Supplier's sub-contractor which are joined together so that they can exchange information in a segregated environment.
Supplier Systems	means system or systems that host Company Data whether they are under the ownership of the Supplier or a Supplier Company or any affiliated sub-contractors.
Supplier's Key Security Contact	means supplier contact with responsibility for the information security of the services, physical security of assets and notification and update on business continuity invocation in the event of a business continuity incident.
Testing Environment	means environment made available for the testing of recently developed programs or software products prior to being released into a Production Environment.

1. INTRODUCTION

1.1. Subject to the provisions set out below, the Supplier shall be responsible for all aspects of the security of the Services and shall take action to safeguard the Services against:

1.1.1. breach of confidentiality (e.g. unauthorised observation, acquisition or transmission of paper or electronic data including voice);

1.1.2. loss of integrity of information either in storage or in transit (e.g. loss, corruption, contamination or obliteration of data including voice);

1.1.3. loss of availability of information due to failure or compromise of the Services;

1.1.4. unauthorised access to, use of, or interface with the Services by any person;

1.1.5. unauthorised breaches of physical security, including network elements, buildings and tools used by the supplier in the provision of the Services; and

1.1.6. use of the Services by any Third Party (including, but not limited to, a sub-contractor) in order to gain access to any computer resource of an authorised user unless the Company has explicitly permitted this in writing.

1.2. The Supplier must ensure that its Information Security Controls where applicable to the Services provided to the Company:

1.2.1. are contained within an up-to-date information security policy which is approved by the Supplier's management, published and communicated to all personnel;

1.2.2. meet all local and Applicable Security Law Requirements;

1.2.3. are substantially aligned with the information security requirements documented within the international ISO27001 standard; and

1.2.4. are compliant with this Schedule and accept that the requirements within it are subject to change to ensure continued protection of any Group Company and their respective clients and customers.

1.3. The Supplier will appoint an appropriate individual to act as the Supplier's Key Security Contact to:

1.3.1. act as the first point of contact for all the Company information security, physical security and BCM related questions, requests, issues and incidents;

1.3.2. attend all relevant meetings;

1.3.3. have or have access to Subject Matter Expertise in information security; and

1.3.4. either have authority to approve any technical or procedural changes required to maintain the security of the services or access to appropriate escalation routes within the Supplier's organisation to obtain prompt approval.

2. INFORMATION SECURITY RIGHT OF AUDIT

2.1. The adequacy of the Supplier's Information Security Controls will be periodically assessed (save in the case of a reasonably suspected breach by the Supplier of its obligations under this Appendix 6 or following any significant security breach) either by:

2.1.1. a direct on-site or remote assessment by the Company information security SMEs or an independent sub-contractor under the Company's general rights of audit under the Agreement; no more than once annually or

2.1.2. an ISAE3402, SSAE16, ISO/IEC27001:2022, PCI DSS v4.0 or other appropriate audit of Information Security Controls ordered by the Supplier and conducted by an independent party, but only where:

2.1.2.1. the date of such independent assessment, certification or audit is no more than twelve (12) months prior to the Company's request to assess the Supplier's Information Security Controls;

2.1.2.2. the Company accepts the scope as being adequate to prove Information Security Control standards for all Services; and

2.1.2.3. such output can be shared with the Company (allowing for reasonable redaction and/or appropriate non-disclosure agreements should this raise any issues of confidentiality); and

2.1.2.4. a regular or frequent cyber ratings report conducted and published by a reputable cyber ratings agency, where such output can be shared with the Company or the Company's client upon request.

2.2. The output of any direct on-site, remote or independent assessment must enable the Company to compare the adequacy of the Supplier's Information Security Controls against the standards of security required in the Agreement;

2.3. Where the Supplier's Information Security Controls (as assessed either by the Company or by an independent audit) are deemed to be inadequate, the Company and the Supplier shall agree on a remedial plan and a timetable for achievement of improvements. The Supplier shall notify the Company of remediation completion and shall allow the Company to conduct a further assessment if requested;

2.4. All expenses incurred associated with such an assessment by the Supplier, sub-contractors employed by the Supplier (or as the case may be, a Supplier Company) including all staff expenses of those organisations shall be the responsibility of the Supplier; and

2.5. The Company shall accept responsibility for all expenses incurred by its staff including expenses associated with the use of an independent sub-contractor only.

3. INCIDENT MANAGEMENT

3.1. The Supplier will:

3.1.1. implement a process for the management and reporting of security related incidents or suspected security incidents (including, but not limited to: (i) losses of data storage devices; (ii) destruction of, damage to, theft of, or unauthorised access to any store of the Company Data; and (iii) exploitation of any vulnerability in the Supplier's hosted networks, connections, applications, websites, or servers if such exploitation may impact the security of any the Company Data or otherwise damage the Company's reputation);

3.1.2. provide immediate communication of the actual or suspected security incident to the Company and to all persons accessing the Services in order for the Company to fulfil its obligations of timely notification to the ICO in accordance with GDPR Regulation;

3.1.3. promptly provide the Company with such assistance and co-operation as the Company may request in relation to the conduct of investigations into any confirmed incident which includes the preserving of any evidence if required for forensic analysis; and

3.1.4. test its Security Incident Management Process no less frequently than once in every twelve (12) month period.

4. INFORMATION ASSET MANAGEMENT

4.1. The Supplier shall implement and maintain an asset register which records all hardware, software and data assets, this register includes:

4.1.1. a Supplier owner for each asset; and

4.1.2. a record for each asset which defines its purpose, location and acceptable use in accordance with its information classification.

4.2. Any assets used for the Company Data shall manage information privacy appropriately and have established security controls for handling Personally Identifiable Information.

5. SUB-CONTRACTORS

5.1. Without prejudice to any other provision of the Agreement relating to sub-contracting, inform the Company of any functionality that is sub-contracted and to whom and ensure that:

5.1.1. each sub-contractor complies with all applicable requirements of this Appendix 6;

5.1.2. background verification checks of all Sub-Processors are carried out in accordance with relevant laws, regulations and ethics;

5.1.3. the Information Security Controls of each sub-contractor are regularly checked to confirm that they are adequate and are being operated effectively and that evidence of such checks is retained; and

5.1.4. where requested by the Company, provide the Company with evidence of the Information Security Controls of each sub-contractor to support any assessment, remediation, governance or incident investigation activity conducted pursuant to this Appendix 6.

6. ACCESS CONTROL

6.1. The Supplier will:

6.1.1. maintain and implement appropriate security systems, controls, policies and procedures to ensure the secure use of the Relevant Systems and any the Company Data held therein;

6.1.2. ensure that access to the Relevant Systems is only granted to those Supplier Personnel who reasonably need it for the purposes of delivering the Services;

6.1.3. ensure that access to the Relevant Systems by Supplier Personnel is restricted in accordance with the role or function of the individual and that access is added, modified, deleted and reviewed in a timely manner and in accordance with current policies;

6.1.4. ensure that background verification checks on all candidates for employment are conducted in accordance with relevant laws, regulations and ethics; and

6.1.5. ensure all users are authenticated by using an identifier (e.g., a User ID) and an authenticator (e.g., a password).

7. REMOTE ACCESS SECURITY

7.1. The Supplier shall ensure that controls are in place to prevent unauthorised remote access to the Relevant Systems. Such controls shall include, without limitation:

7.1.1. any remote access to Relevant Systems shall use industry approved remote access tools and strong authentication;

7.1.2. all data travelling across a remote access mechanism shall be encrypted from the end-point (e.g. laptop) to the network;

7.1.3. all attempts to connect to the Relevant Systems using an unauthorised remote access mechanism shall be rejected and logged; and

7.1.4. all such remote access logs shall be reviewed, and any suspicious activity investigated.

8. CUSTOMER ACCESS TO THIRD PARTY SYSTEMS

8.1. The Supplier will ensure that all aspects of individual customer access to the organisation's business applications meet security requirements by:

8.1.1. maintaining a documented standard or procedure for the provision of customer access to the organisation's business applications;

8.1.2. controlling the means of authentication to ensure each customer is uniquely identified, type of access is appropriate and maintain a record of all authentication activity; and

8.1.3. installing a single point of contact or call centre for handling customer access queries or security issues.

9. THIRD PARTY ACCESS & SYSTEM MAINTENANCE TO COMPANY SYSTEMS

9.1. The Supplier shall ensure that any and all access to any Company Systems by any sub-contractor or the Supplier (or, as the case may be, of a Supplier Company) including to perform maintenance, either on site or remotely will:

9.1.1. be covered by an active contract between the Supplier (or the applicable Supplier Company) and applicable Sub-contractor which contains non-disclosure provisions no less robust than the non-disclosure provisions set out in this Agreement before access is provided;

9.1.2. is approved in advance in writing by the Company and managed in tandem with an assigned Company or Company employee and is restricted to specified individuals only;

9.1.3. has defined objectives and scope agreed with appropriate Company supplier relationship personnel prior to the commencement of any planned Maintenance and Support activities;

9.1.4. restricts access rights to the minimum level required to perform the Maintenance and Support activities and disables access rights immediately following completion of those activities; and

9.1.5. is reviewed and revalidated on a regular basis to ensure that, inter alia, any access no longer required is removed in a timely manner.

10. STAFF SECURITY, TRAINING AND AWARENESS

10.1. The Supplier shall ensure that all persons accessing the Relevant Systems are screened prior to employment, trained in and aware of the provisions of this Appendix 6 and their responsibilities by:

10.1.1. ensuring that robust background verification checks on all candidates for employment are conducted in accordance with relevant laws, regulations and ethics;

10.1.2. documenting information security responsibilities for all employees throughout the organisation which include security responsibilities in job descriptions and terms and conditions of employment; and

10.1.3. providing induction training for all new employees and ongoing training for all staff with specific coverage of information security.

11. MEDIA AND MOBILE DEVICE SECURITY

11.1. The Supplier will:

11.1.1. not store Company Data on unencrypted portable storage devices such as external hard drives, USB sticks, laptops or portable backup media;

11.1.2. not store Company Data on any personally owned mobile or smartphone devices;

11.1.3. ensure that any corporately owned mobile or smartphones devices are appropriately approved, password protected, encrypted and configured to prevent unauthorised access; and

11.1.4. ensure that all Company Data held on removable media (disks, memory sticks, etc) is encrypted using at least AES 128bit.

12. DATA TRANSFER SECURITY

12.1. The Supplier will ensure that:

12.1.1. all Company Data sent over any email system has appropriate Transport Layer Security (TLS) in place;

12.1.2. all Company Data sent over the internet using any known internet protocols (e.g. FTP, SMTP) is encrypted using a minimum AES 128bit encryption mechanism whilst in transit; and

12.1.3. instant messaging over external networks and text messaging is not used to communicate Company Data.

13. CRYPTOGRAPHIC CONTROLS

13.1. The Supplier shall implement appropriate cryptographic controls to ensure that:

13.1.1. the confidentiality of all Company Data is protected using industry recognised appropriate encryption strength and algorithms, both in transit and at rest; and

13.1.2. only trusted keys and certificates are accepted, and that the protocol in use only supports secure versions, with approved length and with appropriate generation and management of those keys.

14. DATA STORAGE & DISPOSAL

14.1. The Supplier shall ensure that:

14.1.1. all information is secured under lock and key if left unattended by Supplier Personnel and its access is appropriately restricted;

14.1.2. any IT assets and electronic media that are being used to store only Company Data but which are no longer required are destroyed by incineration or damaged beyond repair by an industry recognised method;

14.1.3. all electronic Company Data is erased using data erasure technology that confirms it is not recoverable; and

14.1.4. any paper documents containing Company Data which are no longer required are disposed of by shredding, using a third-party data disposal organisation or appropriate internal disposal means.

15. SYSTEM DEVELOPMENT LIFECYCLE (SDLC) SECURITY

15.1. The Supplier will operate a robust System Development Lifecycle (SDLC) which includes information security requirements that must be implemented on all software elements supporting the Service, ensuring that:

15.1.1. there is clear segregation of environments between all environments, including but not limited to, Development Environments, Testing Environments and Production Environments;

15.1.2. developers have no access to any Production Environments and are not able to promote code to any Production Environments;

15.1.3. all system changes affecting project and support environments are reviewed to ensure that they do not compromise the security of those environments;

15.1.4. all system changes and associated code is approved by the appropriate Supplier manager prior to the deployment of any such change to the Production Environment;

15.1.5. secure coding standards are documented, followed and appropriately reviewed prior to deployment;

15.1.6. source code, including all software under development, is appropriately controlled including being securely stored, version controlled, protected from unauthorised access and fully tested in a lesser environment prior to deployment to any Production Environment; and

15.1.7. no Company Data classified as 'RESTRICTED' or 'CONFIDENTIAL' is stored or used at any time in any Development or Test Environment.

16. THIRD PARTY NETWORK MANAGEMENT

16.1. The Supplier will take all steps necessary to safeguard the security of their network through:

16.1.1. restricting access to the network to only Supplier Personnel approved in advance by an appropriate manager within the Supplier's organisation to access any Supplier Network;

16.1.2. implementing controls which ensure that any Supplier Network is used only for its intended business purpose;

16.1.3. configuring network devices (including routers, switches and firewalls) to ensure they do not compromise the security of the network;

16.1.4. creating specific firewall rules that control and limit the level and type of network activity which are routinely reviewed and changed only via change request including approval by an appropriate network manager;

16.1.5. implementing network logging and monitoring capability which includes, but is not limited to, logging of all unauthorised authentication attempts; and

16.1.6. limiting remote maintenance of Supplier Systems and Networks to only essential maintenance by authorised individuals confined to individual sessions.

17. THIRD PARTY APPLICATIONS

17.1. The Supplier shall ensure that any and all Supplier Systems used by the Supplier or any sub-contractor for the purposes of providing Services to the Company will:

17.1.1. be appropriately segregated from other internal or untrusted networks;

17.1.2. have appropriate, and up to date, security controls such as patches, encryption, firewall protection and Anti-Virus where relevant;

17.1.3. limit access to a least privilege principle for all internal and external employees;

17.1.4. follows appropriate password configuration and management guidelines, including but not limited to instructing employees to:

17.1.4.1. keep passwords or memorable words confidential by not sharing with any other person, writing passwords down or storing them in any IT function or facility;

17.1.4.2. change passwords immediately if there is an actual or suspected breach of password security;

17.1.4.3. regularly change passwords as required by the Company Systems to maintain security; and

17.1.5. not access, use or attempt to access or use the Company Systems using any other person's credentials.

17.2. Passwords will be automatically revoked after five (5) consecutive unsuccessful log-on attempts. Resetting of passwords where revoked or forgotten will be carried out as determined by the Company from time to time.

18. THIRD PARTY INFRASTRUCTURE

18.1. The Supplier will have appropriate operating procedures for the management and operation of all information processing facilities, including e-commerce environments by:

18.1.1. maintaining policies and procedures for system maintenance;

18.1.2. standardised system builds for all Supplier Systems and Supplier Network devices;

18.1.3. conducting regular logging and monitoring of all information security events and user activity on Supplier Systems which detects any unauthorised access, modification or deletion of data;

18.1.4. implementing a secure wireless solution which ensures that all requirements are authorised, authenticated, restricted appropriately and protected from unauthorised access; and

18.1.5. implementing appropriate encryption for all wireless traffic.

19. PATCHING AND ANTI-MALWARE

19.1. The Supplier will have a centrally managed anti-malware solution. Anti-malware protection will be in place on all devices used at any time to store or process Company Data and malware signatures on any network connected device will include latest updates from the anti-malware vendor at all times.

19.2. The Supplier will have a process for dealing with actual or suspected malware infections to ensure that any potential or actual security breaches linked to infections are promptly investigated and notified to the Company.

19.3. The Supplier will have a process for:

19.3.1. identifying and risk-assessing all new patches made available for systems storing or processing Company Data;

19.3.2. the timely testing and implementation of patches in non-Production Environments;

19.3.3. authorising implementation of patches before they are applied to production systems;

19.3.4. rolling back implemented patches without operational impact on Services if required; and

19.3.5. maintaining records of all patching activities.

20. INTRUSION DETECTION

20.1. The Supplier will operate appropriate Intrusion Detection mechanisms for all and any Supplier Systems and Supplier Networks to identify predetermined and new types of attack.

20.2. Intrusion Detection methods should be supported by documented standards or procedures;

20.3. Intrusion Detection mechanisms should identify activity typically associated with malware or traffic originating from known malicious IP addresses or network domains, known attack characteristics or unusual or anomalous behaviour; and

20.4. Intrusion Detection mechanisms should be configured to incorporate new or updated attack characteristics, provide alerts when suspicious activity is detected, and allow for suspected intrusions to be analysed and potential business impact assessed.

21. WEB SERVICES SECURITY

21.1. The Supplier will:

21.1.1. conduct penetration testing, on an annual basis or after any significant change, of any interfaces to be used by the Company, the clients and customers of the Company or of any Group Company. In respect of such penetration testing, the Supplier will:

21.1.1.1. ensure that the scope is agreed with the Company;

21.1.1.2. ensure that the penetration testing supplier is agreed with the Company;

21.1.1.3. where a penetration test is conducted by the Supplier, provide the Company with a copy of the report which confirms the penetration testing company used, date of the test, scope and key findings; or

21.1.1.4. allow the Company to perform its own penetration testing where the Supplier either does not perform its own testing or does not perform it to a level acceptable to the Company.

21.1.2. conduct regular vulnerability scans of all:

21.1.2.1. internet-facing interfaces;

21.1.2.2. internal systems that store or process Company Data; and

21.1.2.3. network components (including, but not limited to, firewalls) that protect systems storing or processing Company Data;

21.1.3. ensure that any output of the vulnerability scans is made available to the Company for scrutiny upon request;

21.1.4. ensure that any vulnerabilities identified are remediated and that any associated risks are properly articulated and effectively managed; and ensure that any vulnerabilities identified that cannot or will not be remediated are communicated to the Company with appropriate explanation.

22. PUBLIC CLOUD SERVICES

22.1. The Supplier will:

22.1.1. not store, host, or process any Company 'RESTRICTED' or 'CONFIDENTIAL' information in any Public Cloud Service without the prior written consent of the Company;

22.1.2. provide adequate assurance of the Public Cloud Services provider's security controls by allowing the Company access to any or all of the following:

22.1.2.1. documentation relating to the Supplier's due diligence activity in respect of the Public Cloud Services provider;

22.1.2.2. ISAE 3000, ISAE 3402, SSAE16 or any similar independent SOC II audit of the Public Cloud Services provider; and

22.1.2.3. where applicable, details of the scope and certification status of ISO/IEC 27001:2022.

23. PAYMENT CARD INDUSTRY – DATA SECURITY STANDARDS

23.1. Where end user initial or full payment for Goods and/or Services is made using a debit or credit card, the Supplier will ensure (and will procure that any sub-contractor ensures) that the Services (and any component thereof) are compliant with the latest Payment Card Industry Data Security Standard version and will, upon request, provide to the Company evidence demonstrating compliance with this Clause 23.

24. CONTRACT EXPIRY

24.1. Without prejudice to any other provisions of this Agreement regarding the consequences of termination and/or exit (and in addition to those provisions), upon the expiry or termination of this Agreement, the Supplier shall:

24.1.1. assist the Company in performing a termination review detailing the nature, type and classification of Company Data held within the Supplier, Supplier Company (or, as the case may be, of a Supplier Company's) sub-contractors network and the requirement to retain any the Company Data following Agreement expiry or termination;

24.1.2. assist the Company in the system extraction, packaging and return (in a format mutually agreed) and/or destruction of all the Company Data from all sources, networks and devices;

24.1.3. ensure that all physical or logical assets, intellectual property and licences are returned, and physical and logical system access to the Company Data or the Company Systems is revoked within timescales agreed with the Company;

24.1.4. confirm in writing to the Company that the Company retains the right to perform a periodic assessment of the Supplier to confirm the adequacy of the Supplier's Information Security Controls, where Company Data is retained post contract expiry no more than once annually (pursuant to Clause 3.1 of this Appendix 6); and

24.1.5. provide appropriate notification and assistance to the Company should a data breach occur where Company Data is directly or indirectly impacted (pursuant to Clause 3 of this Data Security Appendix).

25. PHYSICAL SECURITY MANAGEMENT

25.1. The Supplier shall be responsible for all aspects of the physical security in relation to the Services provided, Company Assets whether they reside with the Suppliers operating facility, Supplier Company's (or as the case may be, of a Supplier Company's) sub-contractor logical or physical premises and shall ensure that:

25.1.1. appropriate Physical Security Controls will be implemented in order to protect all Company Assets whilst in their possession, custody or control and shall take action to safeguard them;

25.1.2. its Physical Security Controls are aligned with the physical security requirements in international standard ISO/IEC27001:2022 as a minimum; and

25.1.3. the Company are informed promptly upon identification of any Physical Security Incident which could cause an exploitable vulnerability to the physical security profile of the Company or any other company within the Company's Group, and will provide the Company with such assistance and co-operation as the Company may reasonably request in relation to the conduct of any investigation into any Physical Security Incidents.

26. BUSINESS CONTINUITY MANAGEMENT

26.1. The Supplier shall have a documented Business Continuity Management Programme and associated Business Continuity Plans enabling it to restore Goods and/or Services to an acceptable predefined level should a Business Continuity Incident occur and shall ensure that:

26.1.1. each Business Continuity Plan is reviewed and approved by the Supplier's senior management at least annually;

26.1.2. both the Business Continuity Management Programme and associated Business Continuity Plans reflect relevant regulations and guidance issued by the appropriate regulatory authority and shall be managed to a standard no lower than ISO22301;

26.1.3. all Business Continuity Plans shall have clearly documented Business Impact Analysis, Recovery Time Objectives, Recovery Point Objectives and Minimum Business Continuity Objective;

26.1.4. all Business Continuity Plans are exercised at least annually, the Company informed of the dates of planned exercises and the results and corrective action plans made available to the Company upon request;

26.1.5. all relevant staff are appropriately trained to recognise what a Business Continuity Incident is, and are familiar with the conditions on which a Plan will be invoked, and suitably trained in the steps required to enable the recovery solution; and

26.2. the Supplier shall notify the Company immediately of any potential invocation of the Business Continuity Plan, provide ongoing updates to the Company in line with the agreed escalation process and provide a post incident report within forty-eight (48) hours of the Services being resumed outlining all steps undertaken during invocation.

The parties have signed this Agreement on the date set out above.

SIGNED for and on behalf of [***Insert name of Tag entity.***]

……

SIGNED for and on behalf of [***Insert Supplier name***.]

……