Information Security and Risk Management Policy - Version 10 (V10)

Uncontrolled when printed

Contents

Information Security and Risk Management Policy - Version 10 (V10) 1
1. Definitions and Interpretation 2
2. General Provisions and Scope 7
3. Information Security Management and Accountability 8
4. Information Security Compliance, ISMS and Assurance 8
5. AI Regulatory Compliance and AI Governance 9
6. Information Processing and Handling 13
7. Access to the Company's Systems Environment 15
8. Supplier Technical Security Controls 16
9. Encryption and Cryptographic Controls 18
10. Secure Disposal and Return of Company Materials 18
11. Information Security Incidents and Breaches 19
12. PCI DSS 21
13. Operational Technology Security 21
14. Vulnerability and Patch Management 22
15. Secure Software Development 24
16. Software Supply Chain Security 26
17. Secure AI Development and Operation 26
18. Logging and Monitoring 27
19. Physical Security 29
20. Awareness and Training 29
21. Subcontractor Security Management 30
22. Business Continuity, Disaster Recovery and Operational Resilience 31
23. Governance, Records, Reporting and Audit 32
24. Control Exceptions, Risk Acceptance and Material Change 33
25. Insurance 33

1. Definitions and Interpretation

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

Term	Definition
Agreement	As defined in the front-end agreement between the Company and the Supplier to which this Policy is annexed. Where not defined, this means the agreement (including all schedules, appendices and order documents) under which the Supplier supplies the Goods and/or Services.
AI or Artificial Intelligence	Machine-based technologies capable of generating outputs, predictions, recommendations, decisions, content or other results with a degree of autonomy, including machine learning systems, generative AI systems, automated decision-making systems and AI agents. References to AI include, where applicable, AI Systems, Service AI Systems and AI Technology.
AI Bill of Materials (AIBOM)	A maintained inventory of the AI components, models, datasets, dependencies, tools, prompts, third-party services, model versions, provenance, licensing information and integration points used within a Service AI System.
AI Incident	AI Incident means any event where a Service AI System materially deviates from documented or intended behaviour, produces unlawful, harmful, biased or misleading Outputs, or fails a safety, bias, security or AI governance control, or where any other AI System processes Company Materials other than as permitted under this Policy. An AI Incident shall be treated as an Information Security Incident under this Policy and notified without undue delay, and in any event, in accordance with Section 11 (Information Security Incidents and Breaches).
AI Laws	All laws, regulations and binding regulatory requirements (including relevant data protection laws) applicable to the development, provision, deployment, operation or use of AI Systems or AI Technology in connection with the Goods and/or Services, including the EU AI Act where it applies as a matter of law.
AI System	A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate Outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. This definition shall be construed consistently with Article 3(1) of the EU AI Act.
AI Technology	Any model or model family, algorithm, architecture, dataset, pipeline, embedding, vector database, runtime component, API, safety or evaluation tooling, deployment platform, hosting environment, cloud infrastructure, compute resources, compute provider or compute infrastructure used to build, train, fine-tune, deploy, operate, monitor or govern an AI System.
Auditor	As defined in the Agreement. Where not defined in the Agreement, this means: the Company, its internal auditors, external auditors, professional advisers, regulators, customers (where contractually permitted) or any third party appointed by the Company to assess compliance with the Agreement or this Policy.
Business-Critical Service	Any Goods and/or Services that support critical business operations, regulated activities, customer-impacting services, essential functions, Operational Technology, payment services, personal data processing, or other services identified by the Company as business-critical.
Chief Security Officer or CSO	A party's Chief Security Officer or authorised representative. For the Company, this means the Group Chief Security Officer or authorised delegate.

Cloud Services	Computing infrastructure, platforms, systems, software, storage, applications or related resources delivered remotely by the Supplier or by a third-party cloud service provider acting on behalf of or in coordination with the Supplier, including IaaS, PaaS and SaaS.
Company	As defined in the Agreement. Where not defined in the Agreement, this means: Centrica plc or the relevant Centrica group entity that is a party to the Agreement and receives the Goods and/or Services under the Agreement.
Company-Dedicated Environment	Any environment, tenant, instance, partition or logical segment of a system or platform operated by or on behalf of the Supplier or any Subcontractor, whether single-tenant or multi-tenant, in which Company Materials are stored or processed or through which the Goods and/or Services are configured or administered for the Company.
Company Materials	All Company Data, together with all other documents, data, information, records, specifications, software, hardware, equipment, tools, credentials and Intellectual Property Rights provided by or on behalf of the Company to the Supplier or its Subcontractors, and all prompts, inputs, embeddings, vector representations, telemetry, logs, Outputs or derivative materials generated in connection with the use of Company Data in any AI System or AI Technology, in each case in any form or medium. Company Materials includes any materials derived from, incorporating, or created by any modification, enhancement or development made using any of the foregoing.
Company's Systems Environment	The information technology, Operational Technology, systems, networks, applications, databases, platforms, cloud environments, interfaces, devices and related components owned, operated or controlled by the Company, or operated on its behalf, that process, store, transmit, manage or support Company Materials or Company business operations.
Control Exception	Any non-compliance, deviation, temporary waiver, compensating control arrangement, risk acceptance or inability to meet any requirement of this Policy or the Agreement.
Endpoint Software	Software, including agents, sensors, plug-ins and browser extensions, provided by or on behalf of the Supplier or any Subcontractor for installation or execution on devices managed by or on behalf of the Company.
Facility or Facilities	Any office, building, site, premises, data centre, contact centre, operational location, storage facility or other physical location used by or on behalf of the Supplier or its Subcontractors to house any Company Materials, Supplier Personnel or the Supplier's Systems Environment, or otherwise used in connection with the Goods and/or Services or the Supplier's obligations under the Agreement.
Good Security Practice	Security practices that are documented, risk-based, approved through appropriate governance, operationally embedded, monitored, reviewed and improved in accordance with Good Industry Practice, applicable laws and regulations, recognised standards and relevant Company requirements, including ISO 27001, ISO 27017, NIST, NCSC guidance, OWASP, CIS and IEC 62443 where applicable.
Goods and/or Services	As defined in the Agreement. Where not defined in the Agreement, this means: any goods, products, software, systems, platforms, applications, deliverables, professional services, managed services, support services, consultancy services, cloud services, operational services or other products or services supplied, developed, operated, maintained or provided by or on behalf of the Supplier under the Agreement.

High-Risk AI System	A Service AI System classified as high risk under applicable law or regulations, including the EU AI Act, or that involves processing likely to result in a high risk to the rights and freedoms of individuals under data protection laws (including where a data protection impact assessment is required), or as determined by the Company or Supplier based on potential impact to safety, fundamental rights, regulated activities, customers, critical operations, Company Materials or business-critical processes. The Supplier shall notify the Company promptly upon identifying, or becoming aware of any circumstances indicating, that a Service AI System is or may be a High-Risk AI System. A determination by the Supplier shall be effective without the agreement of the Company. A determination by the Company shall be made acting reasonably and, where practicable, following consultation with the Supplier, and shall take effect from the date notified. Where such determination materially increases the Supplier's costs or obligations, the parties shall discuss in good faith any consequential changes under the Change Control Procedure, provided that the Supplier shall comply from the date notified unless and until otherwise agreed in writing.
Information Risk	Any physical, logical, technical, organisational, operational, Supplier, privacy, cyber, resilience, AI, OT, regulatory or compliance risk that could negatively impact the confidentiality, integrity, availability, authenticity, accountability or non-repudiation of Company Materials, the Company's Systems Environment, the Supplier's Systems Environment, the Goods and/or Services or the Company's operations.
Information Security Breach	Any Information Security Incident, event or circumstance in which the Supplier or the Company becomes aware of, or reasonably suspects, a compromise of information security, physical security, operational security, confidentiality, integrity, availability, data protection, regulated data, Company personal data, Company Materials, Company systems, Supplier systems, Facilities, AI Systems, OT environments or any Goods and/or Services.
Information Security Incident	One or more unexpected, undesired or suspicious physical or logical events that affect the Supplier's Systems Environment, the Company's Systems Environment, Company Materials or the Goods and/or Services and that indicate actual or potential compromise, control failure, vulnerability, unauthorised activity, operational disruption or security weakness.
Information Security Management System or ISMS	The integrated governance structures, policies, standards, procedures, processes, controls, technologies, roles and assurance activities established and maintained by the Supplier to manage Information Risk and protect information assets throughout their lifecycle, and shall include any policies, standards and controls defined or maintained by the Company that the Supplier is required to comply with under the Agreement or this Policy.
Information Security Manager	The individual appointed by the Supplier who is responsible for ensuring the Supplier's compliance with this Policy.
Location Statement	Has the meaning given in paragraph 6.8.
Malicious Software	Any software, code, script, or program that is designed or intended to cause harm, unauthorized access, disruption, or damage to data, systems, networks, or services. This includes, but is not limited to, viruses, worms, trojan horses, ransomware, spyware, adware, rootkits, logic bombs, and any other type of code or software that exhibits malicious behaviour or compromises the confidentiality, integrity, or availability of information or systems.
Material Change	Any change that may affect the security, resilience, compliance, architecture, hosting, data processing, location, Subcontractor support, use or operation of

	any Service AI System, access arrangements, connectivity, control environment, assurance posture or risk profile of the Goods and/or Services.
Material Subcontractor	Any Subcontractor whose services, systems, Supplier Personnel, Facilities or processes are necessary for the delivery of the Goods and/or Services and whose failure, disruption, or unavailability could reasonably be expected to have a material adverse impact on the availability, continuity, recovery, security, compliance, or performance of the Goods and/or Services.
Operational Technology or OT	Hardware, software, networks and systems used to monitor or control physical devices, processes and events in industrial or operational environments, including ICS, SCADA, DCS, PLCs and related embedded or safety-supporting systems.
Outputs	All content, artefacts, data or results generated by or through an AI System, including text, code, images, audio, video, predictions, recommendations, datasets, scores, decisions or derivative materials.
Payment Card Data	Payment card account data as defined by the PCI SSC, including all Cardholder Data (CHD) and Sensitive Authentication Data (SAD).
PCI DSS or Payment Card Industry Data Security Standard	The Payment Card Industry Data Security Standard as published and updated from time to time by the PCI Security Standards Council.
PCI In Scope Services	Any Goods and/or Services that collect, store, process, transmit, or facilitate Payment Card Data, or that could directly or indirectly affect the security of Payment Card Data or the Company's compliance with PCI DSS (e.g. hosting, WAF, APIs, CDN, managed services).
PCI QSA or Payment Card Industry Qualified Security Assessor	A Qualified Security Assessor qualified in accordance with the procedures and requirements established by the PCI Security Standards Council.
PCI SSC or Payment Card Industry Security Standards Council	The Payment Card Industry Security Standards Council, being the organisation responsible for developing, maintaining and promoting PCI DSS and related payment card security standards.
Policy	This Information Security and Risk Management Policy
Regulatory Authority/Regulatory Authorities	As defined in the Agreement. Where not defined in the Agreement, this means: Any governmental, regulatory, supervisory, law enforcement, judicial or other competent authority having jurisdiction over the Company, the Supplier, the Goods and/or Services, Company Materials or activities performed under the Agreement.
Remote Access	Any physical or logical connection to the Supplier's Systems Environment or the Company's Systems Environment which is made, or is capable of being made, from outside that environment by any individual, computer, network or Software, and which facilitates or otherwise enables access to Company Materials, the Company's Systems Environment, the Supplier's Systems Environment or the Goods and/or Services, including any connection intended to provide remote access or remote working.
Security Defect	The presence of Malicious Software, defect, misconfiguration, vulnerability, unauthorised change, insecure design, unsupported component, control weakness or exploitable condition in Software, AI Systems, APIs, infrastructure, Supplier systems or service delivery arrangements that may compromise information security.

Security Incident Management Plan	The documented policies, standards, procedures, playbooks, governance arrangements, escalation processes and operational activities established and maintained by the Supplier to identify, assess, record, investigate, contain, respond to, recover from, report and learn from Information Security Incidents and Information Security Breaches in accordance with Good Security Practice, and in compliance with any relevant Company-defined policies, standards and controls notified to the Supplier.
Service AI System	Any AI System or AI Technology that: (a) processes Company Materials; (b) generates deliverables or Outputs for the Company; (c) is embedded within or forms part of the Goods and/or Services; or (d) materially influences the delivery, operation, management, monitoring or performance of the Goods and/or Services; but excludes standard administrative, productivity, document management or similar internally operated tools operated internally by the Supplier, provided that such tools i) do not generate deliverables or Outputs for the Company, (ii) do not materially affect the delivery, operation or performance of the Goods and/or Services; and (iii) are used in accordance with paragraph 6.12.
Software	Any software program or code (including any 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 its intent or purpose, and which is, or can be made to be, executable, together with the associated system files, configuration files, scripts and templates used by the Company and/or the Supplier in connection with the Goods and/or Services.
Subcontractor	Any third party, affiliate, service provider, cloud provider, consultant, subcontractor, supplier or other person (including any other member of the Supplier's group) engaged by the Supplier or its Subcontractors to support, deliver, host, operate, process, access, enable or otherwise contribute to the Goods and/or Services, including any third party engaged to provide, host, operate, support or enable any AI System, AI Technology, foundation model, model family, AI service or AI functionality used in connection with the Goods and/or Services.
Supplier	As defined in the Agreement. Where not defined in the Agreement, this means: the party supplying the Goods and/or Services under the Agreement.
Supplier Personnel	Any employee, worker, contractor, consultant, agency worker, temporary worker, secondee or other individual engaged by or on behalf of the Supplier or its Subcontractors in connection with the delivery, support, operation or management of the Goods and/or Services.
Supplier's Systems Environment	All information systems, Cloud Services, Software, APIs, infrastructure, networks, end-user devices, service management platforms, data stores, AI Systems, OT interfaces and related components owned, controlled, operated or used by or on behalf of the Supplier or its Subcontractors in connection with the Goods and/or Services.
Training Data	Any data used to train, fine-tune, validate, test, evaluate, align or improve any AI System. Training Data shall not include Company Materials unless the Company has given express prior written authorisation.

1.2 For the purposes of this Policy, the definitions set out in this Policy shall apply. Capitalised terms used but not defined in this Policy shall have the meanings given to them in the Agreement. Where a term is defined in both this Policy and the Agreement, the definition in this Policy shall prevail for the purposes of

the information security and AI provisions, and the definition in the Agreement shall prevail for the purposes of the warranty, indemnity, intellectual property and liability provisions.

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

1.4 Where this Policy refers to the terms “shall” or “must”, they indicate a mandatory obligation unless expressly stated otherwise.

1.5 Where this Policy refers to requirements being applied "where applicable", "where appropriate", "where practicable", "proportionate to risk" or similar terminology, such application shall be determined having regard to the nature of the Goods and/or Services, service criticality, Company Materials processed, data classification, regulatory obligations, connectivity to the Company's Systems Environment, exposure to external networks, privacy risk classification, AI risk classification, Operational Technology safety impact, threat environment and any Company-approved risk acceptance or Control Exception. Such terms shall not relieve the Supplier of compliance with this Policy where the relevant risk factors indicate that the control is necessary to protect Company Materials, the Company's Systems Environment or the Goods and/or Services.

1.6 References to the Supplier include its Subcontractors, Supplier Personnel, Affiliates, agents and any third parties involved in delivering the Goods and/or Services, unless the context requires otherwise.

2. General Provisions and Scope

2.1 This Policy sets out the Supplier’s information security and artificial intelligence (“**AI**”) obligations in connection with the performance of its obligations under the Agreement.

2.2 This Policy applies where the Supplier or its Subcontractors process, access, store, transmit, support, host, develop, operate or otherwise impact Company Materials, the Company’s Systems Environment, Business-Critical Services, regulated data, customer data, employee data, OT, Service AI Systems, Cloud Services or any Goods and/or Services provided to or for the Company.

2.3 The Supplier shall comply with this Policy throughout the Supplier lifecycle, including onboarding, design, transition, service delivery, change, incident response, assurance, exit, termination and post-termination return or destruction of Company Materials.

2.4 This Policy represents the Company's default contractual information security requirements for applicable supplier engagements. Any deviation, exception, waiver, compensating control or alternative security arrangement shall be subject to the Company's approved governance, assurance and risk acceptance processes and shall not be deemed accepted unless formally approved in writing through the Company's authorised governance route.

2.5 Where there is any inconsistency between this Policy and any other provision of the Agreement relating to information security, privacy, or artificial intelligence, the provision imposing the higher or more protective standard shall prevail, unless the relevant provision of the Agreement expressly identifies the requirement of this Policy from which the parties have agreed to depart.

2.6 The Supplier shall ensure that the Supplier’s Systems Environment, Facilities, Subcontractors, Goods and/or Services are adequately and appropriately secured to avoid or minimise Information Risk.

2.7 The Supplier shall provide written evidence and assurance to the Company on request in respect of the security, resilience and compliance of Company Materials and the Goods and/or Services.

2.8 The Supplier shall continuously assess, manage and improve information security, its ISMS, the Supplier's Systems Environment and any Goods and/or Services provided by or on behalf of the Supplier.

2.9 The requirements of this Policy which are expressed to apply to a Service AI System apply only where, and to the extent that, the Supplier provides, develops, deploys, integrates, hosts, operates, supports, decommissions or otherwise uses a Service AI System. Where the Supplier does not use a Service AI System, such requirements shall not apply unless and until the Supplier proposes to introduce one, at which point they apply with immediate effect and the Supplier shall first comply with paragraphs 5.8 and 5.9. Requirements which are expressed to apply to any AI System or AI Technology apply according to their terms.

3. Information Security Management and Accountability

3.1 The Supplier shall appoint an Information Security Manager responsible for ensuring the Supplier's compliance with this Policy.

3.2 The Supplier shall appoint a suitably qualified deputy or alternate security contact to act when the Information Security Manager is unavailable.

3.3 Before commencing delivery of the Goods and/or Services, the Supplier shall notify the Company of named contacts for security governance, incident escalation, assurance requests, audit activity, vulnerability remediation, AI governance, OT security and business resilience, where applicable.

3.4 The Supplier shall promptly notify the Company of any change to these nominated contacts where such change may affect escalation, assurance, incident handling or service continuity.

3.5 The Supplier shall maintain governance arrangements that ensure information security requirements are owned, monitored, reported and escalated at an appropriate senior level within the Supplier's organisation.

4. Information Security Compliance, ISMS and Assurance

4.1 The Supplier shall institute, operate, maintain, review and improve an ISMS that meets Good Security Practice and incorporates the requirements of this Policy or their substantial equivalent.

4.2 The Supplier's ISMS shall conform to ISO/IEC 27001 or a substantially equivalent standard, appropriate to the Goods and/or Services provided under the Agreement. Where the Supplier uses Cloud Services in connection with the Goods and/or Services, the relevant cloud control environment shall conform to ISO/IEC 27017 or a substantially equivalent standard. Where personal data is processed in Cloud Services, the relevant cloud control environment shall additionally conform to ISO/IEC 27018 or a substantially equivalent standard.

4.3 The Supplier shall create and maintain an ISMS scope statement that includes all Goods and/or Services provided under the Agreement and all relevant systems, people, processes, locations, Subcontractors and data flows.

4.4 The Supplier shall perform and record an Information Risk assessment at least annually and following any Material Change. The assessment shall be conducted in accordance with ISO 27001 or a

substantially equivalent methodology, appropriate to the Goods and/or Services provided under the Agreement.

4.5 The Supplier shall maintain a plan to track identified Information Risks to remediation or formal acceptance (the "**Risk Treatment Plan**").

4.6 The Supplier shall maintain a record of Information Risks, treatment plans, status, ownership, controls, effectiveness, residual risk, accepted risks, overdue actions and target dates (the "**Risk Register**").

4.7 The Supplier shall create, maintain, test and improve a Security Incident Management Plan.

4.8 The Supplier shall demonstrate continuous improvement through corrective actions, lessons learned, audit findings, assurance findings, incident reviews, vulnerability trends, risk treatment progress and control effectiveness reviews.

4.9 The Supplier shall obtain and maintain, for the duration of its obligations under the Agreement, ISO 27001 certification from a nationally accredited certifying body, unless otherwise agreed in writing by the Company.

4.10 The Supplier shall provide formal evidence of certification on request, including an unredacted Statement of Applicability and any associated scope, audit findings or corrective action plans reasonably required by the Company.

4.11 Where ISO/IEC 27001, ISO/IEC 27017/18 or other required certification is not held, the Supplier shall provide equivalent assurance evidence agreed by the Company and document the position as a risk-based exception.

4.12 Assurance evidence may include ISO/IEC certificates, Statements of Applicability, SOC 2 Type II reports, Cyber Essentials (CE) or Cyber Essentials Plus (CEP) evidence where relevant, PCI DSS evidence where applicable, penetration test summaries, remediation evidence, OT assurance evidence, AI assurance evidence, audit reports and control attestations.

4.13 The Supplier shall, where requested by the Company, participate in the Company's approved supply-chain assurance platform, currently Risk Ledger, or any replacement platform notified by the Company, and provide complete, accurate and current security responses, assurance information and supporting evidence. The Supplier shall ensure such information remains current and is updated following any Material Change that may affect the security, resilience, compliance or risk profile of the Goods and/or Services provided under this Agreement.

5. AI Regulatory Compliance and AI Governance

5.1 Where the Supplier provides, develops, deploys, integrates, hosts, operates, supports or decommissions any Service AI System the Supplier shall comply with AI Laws, Company Policies (including, without limitation, this Information Security and Risk Management Policy, the Company's Responsible AI Principles and the Supplier Code of Conduct), Good Security Practice, and shall establish and maintain an AI governance framework aligned to ISO/IEC 42001 or a substantially equivalent standard, and shall have regard to the NIST AI Risk Management Framework, in each case proportionate to the nature, scale and risk of the Service AI System.

5.2 Where the EU AI Act does not apply as a matter of law, the Supplier shall have regard to the principles and requirements of the EU AI Act (and any equivalent or successor legislation) as a reference standard, proportionate to the nature, scale and risk of the relevant Service AI System.

5.3 The Supplier shall also have regard to relevant regulatory guidance and codes of practice applicable to the relevant Service AI Systems, including, but not limited to, guidance and codes issued by Ofgem and the ICO, and any equivalent or successor guidance, in each case proportionate to the nature, scale and risk of the relevant Service AI System.

5.4 The Supplier shall not develop, provide, deploy, operate or support any Service AI System where such use is prohibited under AI Laws. The Supplier shall promptly notify the Company if it becomes aware that a Service AI System is, or may become, subject to a prohibition, restriction or enforcement action under AI Laws.

5.5 The Supplier shall notify the Company without undue delay of any material regulatory investigation, enforcement action, prohibition notice or equivalent regulatory measure relating to any Service AI System.

5.6 The Supplier shall identify and document the role performed by the Supplier, its Subcontractors and, where relevant, the Company in relation to each Service AI System, including whether a party acts as a provider, deployer, importer, distributor or undertakes any other role defined under AI Laws. The Supplier shall maintain a documented responsibility matrix allocating compliance, assurance, monitoring, documentation, incident reporting and evidence obligations to the relevant party and shall provide such information to the Company on request.

5.7 The Supplier shall provide all reasonable cooperation and assistance to the Company in connection with any enquiry, audit or investigation (whether by a Regulatory Authority, the Company or the Company's internal audit or assurance teams) relating to a Service AI System, including providing access to relevant records, personnel, documentation and evidence. This paragraph is without prejudice to, and does not limit, any audit, cooperation, access or assistance obligations of the Supplier under the Agreement or any Data Processing Schedule, which shall prevail to the extent they impose a broader or more onerous obligation.

5.8 The Supplier shall identify, classify and disclose to the Company each Service AI System, including purpose, data inputs, outputs, model provider, hosting location, risk classification, processing of personal data, human oversight arrangements and whether Company Materials are processed. The Supplier shall make such disclosure at the outset of the Agreement, prior to introducing any new Service AI System, and upon any Material Change to a Service AI System or the extent of its use.

5.9 The Supplier shall not introduce, deploy, make available, use, run, train, fine-tune or materially modify any Service AI System, AI functionality, model family, foundation model provider, AI hosting provider or AI use case in connection with the Goods and/or Services unless: (a) the Supplier has provided the Company with reasonable information regarding the proposed use; (b) any Company AI governance review process has been completed; and (c) the Company has approved such use in writing, such approval not to be unreasonably withheld or delayed and to be granted, refused or made conditional within fifteen (15) business days of receipt of the information provided under paragraph 5.9(a). The requirements of this paragraph 5.9 shall not apply to routine like-for-like version updates, patches or security fixes to an approved Service AI System which do not materially change its functionality, behaviour, Outputs, data flows, hosting location or risk profile, provided that the Supplier records such updates and promptly notifies the Company. The Supplier shall procure that its Subcontractors comply with obligations substantially equivalent to those in this Policy and the Agreement, to the extent applicable to the Goods and/or Services.

5.10 Where a change to a Service AI System, model family, foundation model or AI hosting arrangement is made by a third party and not initiated by the Supplier, paragraph 5.9 shall not require prior approval of that change. The Supplier shall instead notify the Company without undue delay on becoming aware of the change, assess its impact on the Goods and/or Services, and propose mitigating measures where the change materially affects performance, functionality, security, regulatory compliance or risk. Continued use of the affected Service AI System following such a change shall remain subject to paragraphs 5.12 and 24.

5.11 The Company may determine, acting reasonably, whether a proposed AI use is approved, approved subject to conditions, or rejected. Where the Company does not approve, or approves subject to conditions, the parties shall discuss in good faith any necessary changes under the Change Control Procedure.

5.12 For the avoidance of doubt, any material change to the behaviour, capabilities, logic or performance of a Service AI System shall constitute a Material Change and shall be governed by paragraph 24 and, where applicable, the AI Change Notice provisions of the Change Control Procedure.

5.13 Upon the Company's request, and no more than annually save where a Material Change or Information Security Incident occurs, the Supplier shall complete and provide to the Company its then-current AI Supplier Questionnaire, or equivalent due diligence documentation, in respect of each Service AI System.

5.14 Before deploying any High-Risk AI System, the Supplier shall complete applicable conformity assessments, maintain comprehensive technical documentation, implement appropriate logging and monitoring capabilities, and establish post-deployment monitoring procedures. The Supplier shall provide evidence of compliance with this paragraph and paragraphs 5.23 and 5.24 to the Company on request. Where the Company is the provider, deployer or other responsible actor in respect of a High-Risk AI System under applicable AI Laws, the Supplier shall provide all information, technical documentation, testing and validation evidence, logs and other assistance reasonably required to enable the Company to complete any conformity assessment, technical documentation, registration, logging or post-deployment monitoring obligation applicable to it, in each case within a reasonable period of the Company's request and in any event within any deadline notified by a Regulatory Authority.

5.15 Where the Supplier provides, integrates, relies upon or makes available General-Purpose AI models (including foundation models), as defined by the EU AI Act, or capabilities in connection with the Goods and/or Services, the Supplier shall maintain appropriate technical documentation, instructions for use, risk assessments, assurance evidence and compliance documentation relevant to such capabilities and shall provide such information to the Company on request, subject to applicable confidentiality, intellectual property and legal restrictions. Where such capabilities are provided by a third party, the Supplier's obligation under this paragraph is to obtain, maintain and make available to the Company the documentation and instructions for use supplied by that third party (including any documentation required to be supplied to downstream providers under AI Laws), together with the Supplier's own documentation of its integration, configuration and use.

5.16 The Supplier shall maintain an AIBOM for each Service AI System and make it available to the Company on request. In respect of components which the Supplier develops, trains, fine-tunes, configures or integrates, the AIBOM shall record full component detail, including datasets, dependencies, tools, prompts, model versions, provenance, licensing information and integration points. In respect of proprietary third-party models and services, the AIBOM shall record the model or service identity, provider, version, hosting location, licence terms and the technical documentation and instructions for use made available by the provider (including any documentation the provider is required to supply to downstream providers under AI Laws).

5.17 The Supplier shall maintain a complete and current inventory of all Service AI Systems, together with the associated model families, foundation models, AI-enabled tools and third-party AI services, and shall provide such inventory to the Company upon reasonable request and at least annually. This inventory is separate from, and additional to, the AIBOM required under paragraph 5.16.

5.18 Where Service AI Systems process personal data, the Supplier shall comply with the Company's relevant data processing schedules and framework, including completing appropriate data protection assessments, applying privacy-by-design and data minimisation, automating decision-making risk assessments, and complying with the Agreement's data processing and cross-border transfer requirements.

5.19 The Supplier shall implement measures proportionate to the risk and use case of the relevant Service AI System, including (as appropriate) human oversight, explainability, transparency, bias and fairness assessment, model monitoring, AI security testing and AI Incident response arrangements.

5.20 Where a Service AI System involves the processing of personal data or automated decision-making, the Supplier shall comply with applicable data protection laws, including requirements relating to automated decision-making and human oversight of such decisions.

5.21 Where Service AI Systems make or materially influence decisions affecting individuals (including where human oversight is required under applicable AI Laws), the Supplier shall: (a) implement and maintain appropriate human oversight mechanisms, having regard to the nature, context and potential impact of the relevant decision; (b) ensure that human reviewers have the necessary competence, authority and access to information to review, validate, override or reverse AI-generated decisions; and (c) provide meaningful, timely and context-appropriate explanations of the logic, significance and consequences of such decisions to the Company and, where required, to affected individuals. Where such decisions are solely automated and produce legal or similarly significant effects on individuals, the Supplier shall not carry out such decision-making without appropriate human intervention in accordance with applicable data protection laws and the prior written approval of the Company's privacy team.

5.22 Where a Service AI System is used to support, inform or make decisions that may affect individuals, the Supplier shall implement appropriate mechanisms to enable concerns regarding the operation, outcome or impact of the Service AI System to be raised and reviewed. The Supplier shall ensure that appropriately qualified personnel are able to investigate such concerns and, on request by the Company, provide a timely and context-appropriate explanation of the relevant AI-assisted decision, outcome or recommendation.

5.23 Prior to the deployment of any new Service AI System, or any material modification to an existing Service AI System, the Supplier shall conduct and document a risk assessment, proportionate to the risk, nature and intended use of the Service AI System, addressing legal, regulatory, privacy, information security, intellectual property, bias, discrimination and operational risks. The Supplier shall provide a summary of such assessment to the Company upon reasonable request. Where such risks materially affect individuals, the Supplier shall also comply with the AI risk and impact assessment obligations in paragraph 5.24.

5.24 Where required by AI Laws, or where a Service AI System materially impacts individuals, the Supplier shall conduct and maintain appropriate AI risk and/or impact assessments over the lifecycle of the Service AI System (including data protection impact assessments where personal data is involved), working in co-operation with the Company where requested, and shall provide summaries or confirmations of completion to the Company upon reasonable request.

6. Information Processing and Handling

6.1 Without prejudice to data protection, confidentiality or other contractual requirements, the Supplier shall ensure Company Materials remain the sole and exclusive property of the Company and are not compromised, lost, destroyed, corrupted, accessed without authority, disclosed without authority or used outside the approved purpose. Nothing in the Agreement, this Policy or the provision of the Goods and/or Services shall grant the Supplier or its Subcontractors any ownership rights or proprietary interest in Company Materials beyond those strictly necessary to perform their obligations under the Agreement.

6.2 The Supplier shall only access, process, store and retain Company Materials to the extent necessary to perform its obligations under the Agreement. This restriction applies to all Company Materials, whether or not comprising personal data, including commercially sensitive and confidential information, and the Supplier shall not process any Company Materials for its own purposes or those of any third party without the Company's prior written approval and completion of the Company's applicable governance and approval processes. In respect of personal data, the consent and governance requirements of the Data Processing Schedule shall prevail.

6.3 The Supplier shall ensure that only Supplier Personnel with a need to know are granted access to Company Materials, and that such access is approved, controlled, monitored and revoked when no longer required.

6.4 The Supplier shall classify, minimise, protect, retain and securely dispose of Company Materials in accordance with Company requirements, applicable legal and regulatory requirements and Good Security Practice.

6.5 The Supplier shall not copy, disclose, transmit, store, access, process or make available Company Materials to any third party or Subcontractor without the Company’s prior written agreement, unless expressly required by law.

6.6 The Supplier shall not store or process Company Materials using public consumer services or unapproved platforms, including personal email, public file-sharing, public AI services or uncontrolled collaboration tools.

6.7 The Supplier shall obtain prior Company approval for any new processing location, storage platform, AI service, Cloud Service, Subcontractor access, cross-border transfer or material change to data handling arrangements.

6.8 Before commencing delivery of the Goods and/or Services, the Supplier shall provide the Company with a written statement (the "Location Statement") identifying:

(a) each Facility, including offices, contact centres and data centres, from which Company Materials are stored, processed, accessed, supported or backed up by the Supplier or any Subcontractor, identifying the relevant Supplier entity or Subcontractor and the activities carried out at each Facility;
(b) each country from which Supplier Personnel, including personnel of any Subcontractor, may access Company Materials or the Company's Systems Environment while working remotely, identifying the relevant Supplier entity or Subcontractor;
(c) for Cloud Services, each cloud provider or Subcontractor used, the hosting regions configured by the Supplier and, where relevant, the countries from which the service is supported, together with a reference to the provider's published processing and support locations; and

(d) each Subcontractor that stores, processes, accesses, supports or backs up Company Materials, or has access to the Company's Systems Environment, together with the services it provides and the locations identified under paragraphs (a) to (c) that apply to it.

The Supplier shall keep the Location Statement complete and current. It shall not appoint a new Subcontractor within the scope of paragraph (d), or store, process, access, support or back up Company Materials from any location not included in the Location Statement, without complying with paragraph 21.3 and obtaining any prior written approval required under paragraph 6.7. Any such approval shall not be unreasonably withheld or delayed and shall be given or refused within ten (10) business days of a complete request. Any temporary approval shall specify its conditions and end date. The Supplier shall request any renewal no later than ten (10) business days before that end date, failing which the approval shall lapse on that date.

Short-term business travel by individual Supplier Personnel (not exceeding 30 days in aggregate in any 12-month period) shall not require approval under this paragraph, provided that: (a) access is from a Supplier-managed device and complies with the Data Processing Schedule and applicable laws; (b) access does not occur from any country or territory subject to UK, EU, UN or US sanctions or export control restrictions applicable to the Supplier or the Company; (c) the Supplier has assessed the relevant location, having regard to Good Security Practice and relevant government travel and cyber-security advisories, and determined, acting reasonably, that such access does not present a materially increased risk to Company Materials or the Company's Systems Environment; and (d) the Supplier maintains a record of such assessments and access and provides it to the Company on request. The Company may, acting reasonably, require the Supplier to cease such access from any location. The Supplier shall remain fully responsible for any access under this paragraph.

This paragraph is without prejudice to paragraph 21.3 or the international transfer and sub-processor requirements of the Data Processing Schedule, which shall prevail in respect of personal data.

6.9 Physical Company Materials shall be protected using appropriate technical and organisational measures and stored securely when unattended.

6.10 Unless expressly authorised by the Company in writing signed by an authorised representative of the Company, the Supplier shall not, and shall ensure that its Affiliates, Subcontractors and any third-party provider do not, use, store, disclose or otherwise process Company Materials to train, fine-tune, validate, test, calibrate, align, evaluate or otherwise improve any AI System or AI Technology, or to develop, improve or commercialise any product or service. On the Company’s reasonable request (and no more than once in any twelve (12) month period, save following an AI Incident, Information Security Breach or Material Change), the Supplier shall provide written certification, signed by an authorised representative, confirming compliance with this paragraph.

6.11 Where the Company authorises any AI training or fine-tuning under paragraph 6.10: (a) such activities shall occur only within a Company-specific and segregated environment; and (b) Company Materials, and any derivatives thereof, shall not be used for any other customer or third-party, or for any internal Supplier purpose.

6.12 Notwithstanding paragraph 6.10, the Supplier, its Affiliates and Subcontractors may use Company Materials with AI functionality embedded in standard administrative, productivity, document management or similar internally operated tools, provided that: (a) such use is necessary in connection with the Goods and/or Services; (b) such use is permitted under the Agreement; (c) Company Materials are not used to train, fine-tune, validate, calibrate, align, evaluate or otherwise improve any AI System or AI Technology; and (d) such AI functionality operates within an enterprise tenancy or equivalent controlled environment under the

Supplier's administrative control, configured to prevent unauthorised access, disclosure or use of Company Materials, and under terms which prohibit the tool provider from using Company Materials to train, fine-tune or improve any AI System or from subjecting them to human review, save where such review is (i) required by law; or (ii) strictly necessary for security, abuse monitoring or service integrity purposes and is carried out under confidentiality and access controls no less protective than those in the Agreement; and (e) the Supplier shall not process any special category personal data, Payment Card Data or other Company Materials classified by the Company as restricted under this paragraph without the Company's prior written approval.

6.13 The Supplier shall not, and shall procure that its Subcontractors and any third-party provider do not, reuse, re-licence, disclose, publish, share or otherwise make available Company Materials, or any derivative thereof, to any third party. This restriction applies to any insights, learnings, parameters, weights, embeddings or statistical representations derived directly or indirectly from Company Materials.

6.14 The Supplier shall not, and shall ensure its Subcontractors do not, reverse engineer, extract, analyse, re-train or otherwise attempt to derive models, weights, embeddings or other learnings from Company Materials.

6.15 Where any AI System is capable of autonomous or semi-autonomous action, including interacting with the Company's systems, data, networks or personnel (directly or via APIs, automated workflows or other system-to-system interfaces), the Supplier shall: (a) disclose such capability to the Company before deployment; (b) ensure the AI System operates under the principle of least privilege, with only the minimum access necessary for its designated function; (c) implement appropriate technical safeguards against prompt injection, data leakage, privilege escalation and unauthorised actions; (d) maintain audit logs and monitoring sufficient to identify the autonomous or semi-autonomous actions taken by the AI System, including the actions taken, the systems and data accessed, and the privileges exercised; (e) implement mechanisms enabling human oversight of, and intervention in, the operation of the AI System, including the ability to review, approve, override or reverse any autonomous or semi-autonomous action; and (f) ensure that the AI System can be suspended, disabled or isolated without undue delay where necessary to protect the Company, Company Materials or the Company's systems, and shall suspend, disable, or isolate promptly on the Company's written request. Logs maintained under paragraph 6.15(d) shall be retained and made available in accordance with Section 18. The Company acknowledges that suspension, disablement or isolation under paragraph 6.15(f) may affect the availability or performance of the Goods and/or Services. Where the Supplier acts on the Company's written request and the request does not arise from the Supplier's breach or default, the Supplier shall not be liable for any failure to meet service levels to the extent directly attributable to that suspension, provided the Supplier uses reasonable endeavours to mitigate the impact and to restore the affected Goods and/or Services promptly following the Company's instruction.

6.16 Where the Supplier uses any AI System, it shall implement technical and organisational measures to logically segregate Company Materials from the data of any other customer and shall not commingle Company Materials with such data. Where commingling is inherent to a third-party AI service and the Company has expressly permitted it in writing, the Supplier shall remain responsible for access controls, encryption and contractual safeguards preventing any access to, or reuse of, Company Materials or any derivative by any other customer.

7. Access to the Company's Systems Environment

7.1 This section applies where the Supplier has any physical or logical connection to, or access to, any systems, software, network, platform, application or environment of the Company.

7.2 The Company shall not grant access to the Company's Systems Environment without prior written approval from the Company's CSO or authorised delegate. Approval may be contingent on the Supplier providing detailed access designs, security controls and assurance evidence for review.

7.3 Where access is approved, the Supplier shall only access the Company's Systems Environment in the approved manner and strictly to the extent necessary to perform its obligations under the Agreement.

7.4 The Supplier shall comply with Company access controls and restrictions, including permitted systems, access methods, permitted locations, authorised users, approved hours of access and any monitoring requirements.

7.5 The Supplier shall apply least privilege, named user accounts, multi-factor authentication, role-based access control, privileged access management and periodic access reviews for Supplier Personnel accessing the Company's Systems Environment.

7.6 Shared accounts, generic accounts or credential sharing are prohibited unless expressly approved in writing by the Company and subject to compensating controls. Emergency, break-glass and temporary elevated access to the Company's Systems Environment shall be managed in accordance with the Company's applicable processes.

7.7 The Supplier shall keep credentials, certificates, tokens, keys and authentication factors strictly confidential and shall not disclose them except to authorised Supplier Personnel for approved purposes.

7.8 The Supplier shall ensure access is promptly removed or suspended when no longer required, including upon role change, termination, contract change, non-compliance or Company request.

7.9 The Supplier shall not attempt to bypass Company controls or resolve access problems in a way that could jeopardise the Company's Systems Environment. Such problems must be reported through agreed channels.

7.10 Supplier Personnel using any part of the Company's Systems Environment shall comply with the prevailing Company Acceptable Use requirements.

8. Supplier Technical Security Controls

8.1 The Supplier shall be responsible for securing the Supplier's Systems Environment, including hardware, Software, Cloud Services, APIs, networks, remote access, endpoints, development environments, Service AI Systems and operational platforms used in connection with the Goods and/or Services.

8.2 The Supplier shall maintain an accurate inventory of assets, systems, APIs, applications, data flows, Software, AI Technology, Cloud Services and Subcontractor services used to deliver or support the Goods and/or Services.

8.3 The Supplier shall implement configuration hardening, secure baselines, vulnerability management, malware protection, endpoint protection, network security controls, secure administration and change control proportionate to risk.

8.4 In respect of systems within the Supplier's Systems Environment, including systems operated by any Subcontractor, that process Company Materials or are used to administer the Goods and/or Services, the Supplier shall implement:

(a) multi-factor authentication for all privileged access, Remote Access and access to Cloud Services administration consoles;
(b) password or passphrase requirements aligned to NCSC guidance, or equivalent recognised guidance, as current at the date of the Agreement, including minimum length, screening against known-compromised credentials, and account lockout or throttling following repeated failed attempts. Default and vendor-supplied credentials shall be changed or disabled before use;
(c) storage of credentials, secrets, keys and tokens in an enterprise password manager, vault or secrets management solution. Credentials shall not be stored in plain text or unencrypted form in code, scripts or configuration files;
(d) privileged accounts that are separate from standard user accounts and are granted on a least-privilege and, where technically practicable, just-in-time or time-bound basis, with privileged sessions logged in accordance with paragraph 18.5; and
(e) review of privileged access at least quarterly, with removal of access no longer required, including standing privileged access to any Company-Dedicated Environment.

The Supplier shall provide evidence of these controls on request, including the outcome of privileged access reviews relating to Company Materials or any Company-Dedicated Environment.

8.5 In respect of systems within the Supplier's Systems Environment, including systems operated by any Subcontractor, that process Company Materials, and any Company-Dedicated Environment, the Supplier shall:

(a) Emergency and temporary elevated access: document and restrict emergency (break-glass) accounts and temporary elevated access. Such access shall be approved, time-limited, vaulted, logged and alerted to the Supplier's security function on use. Associated credentials shall be rotated after each use, and a post-use review completed within five (5) business days. Use of such access affecting Company Materials or a Company-Dedicated Environment shall be reported to the Company in accordance with paragraph 23.11 and on request;
(b) Roles and permissions: maintain a current matrix of the roles and permissions that grant access to Company Materials or any Company-Dedicated Environment, including relevant roles assigned to Subcontractor personnel, and provide it to the Company on request. Any matrix so provided shall be treated as the Supplier's Confidential Information; and
(c) Segregation of duties: define and enforce segregation-of-duties and incompatible-access rules, including segregation between the development, approval and deployment of changes to production. Where such segregation is not reasonably practicable given the size of the Supplier's or relevant Subcontractor's organisation, the Supplier shall implement documented compensating controls approved by the Company in accordance with Section 24.

8.6 The Supplier shall enable and appropriately configure available security and privacy features that are relevant to the Goods and/or Services and necessary to protect Company Materials, having regard to Good Security Practice and the nature and risk of the relevant processing. The Supplier shall maintain records sufficient to evidence the configuration of such features and provide relevant records to the Company on request, where reasonably practicable.

8.7 Remote Access to the Supplier’s Systems Environment or the Company’s Systems Environment shall be authorised, encrypted, authenticated, logged, monitored and limited to what is necessary for the approved purpose.

8.8 The Supplier shall not permit Remote Access that fails to meet this Policy, and shall discontinue, disconnect or prevent any non-compliant Remote Access immediately.

8.9 APIs that process or provide access to Company Materials shall implement strong authentication, proper authorisation, secure input validation, rate limiting, TLS 1.2 or higher, inventory management, logging and monitoring.

8.10 Basic authentication is prohibited for APIs unless expressly approved in writing by the Company and supported by compensating controls.

8.11 Externally accessible web applications that process Company Materials shall meet security verification requirements equivalent to OWASP ASVS Level 2 or higher, be protected by an appropriately configured Web Application Firewall where applicable and undergo penetration testing at least annually and following Material Change.

9. Encryption and Cryptographic Controls

9.1 The Supplier shall implement technical and procedural controls to protect Company Materials regardless of storage location or processing environment.

9.2 Company Materials transmitted electronically outside the Supplier's Systems Environment or across public networks shall be encrypted using encryption aligned to Good Security Practice. Such encryption shall utilise TLS 1.2+, or a substantially equivalent cryptographic protocol providing comparable confidentiality, integrity and authentication protections.

9.3 Company Materials shall be encrypted at rest where required by Company data classification, regulatory requirement, risk assessment or Good Security Practice. Where encryption at rest is required, the Supplier shall utilise AES-256, or a substantially equivalent cryptographic standard providing comparable protection against unauthorised access, disclosure or compromise.

9.4 Encryption algorithms shall maintain confidentiality, integrity and the value of Company Materials throughout their lifecycle and shall align to the Company's applicable policy requirements where applicable.

9.5 The Supplier shall not rely on default or embedded encryption in office productivity tools, online services or compression utilities unless the method meets approved encryption standards and the Company has explicitly approved the use in writing where required.

9.6 The Supplier shall implement key management controls, including secure key generation, storage, access control, segregation of duties, rotation, revocation, backup and destruction.

9.7 Obsolete, insecure or deprecated encryption algorithms shall not be used unless strictly necessary, approved through a documented Control Exception and protected by compensating controls.

9.8 Where insecure or deprecated encryption is identified, the Supplier shall notify the Company without delay, replace the algorithm, re-encrypt affected data where applicable and track remediation through the Risk Register. The Supplier shall be liable for any Information Security Breach arising directly or indirectly from the use of an obsolete, insecure or deprecated encryption algorithm in connection with the Goods and/or Services.

10. Secure Disposal and Return of Company Materials

10.1 The Supplier shall retain Company Materials only for so long as is necessary to perform the Goods and/or Services or as required by applicable law, and in accordance with the Company's data retention

requirements as notified to the Supplier from time to time. The Supplier shall not retain Company Materials for any other purpose or period without the Company's prior written consent. This obligation applies to all Company Materials (whether or not comprising personal data) and is without prejudice to the Supplier's obligations in respect of personal data under the Data Processing Schedule.

10.2 The Supplier shall return, destroy or delete Company Materials when no longer required, when instructed by the Company, on termination or expiry of the Agreement, or on completion of any exit plan. Unless otherwise required by law or expressly agreed in writing by the Company, such return, destruction or deletion shall be completed within thirty (30) calendar days of the relevant trigger event.

10.3 Disposal shall be performed in accordance with Good Security Practice, including recognised secure sanitisation or destruction guidance such as NIST SP 800-88 or equivalent, where applicable.

10.4 Company Materials no longer required shall be treated as confidential waste and protected from unauthorised access until destruction is complete.

10.5 Where Company Materials reside on hardware, media, backups or cloud storage, the Supplier shall ensure secure destruction, deletion or sanitisation prevents subsequent retrieval or restoration, except where retained under approved legal or technical constraints.

10.6 The Supplier shall provide independent verifiable evidence of secure return, destruction, deletion or sanitisation on request, including destruction certificates, deletion attestations or technical evidence where appropriate.

10.7 Where Company Materials have been processed, stored or held in or by any AI System or AI Technology (whether or not a Service AI System and whether or not previously approved by the Company), the Supplier shall, on termination or expiry of the Agreement, on completion of any exit plan, or when otherwise instructed by the Company: (a) cease all processing of Company Materials in all AI Systems and AI Technology; and (b) permanently delete all copies of Company Materials held in or by any AI System or AI Technology, including in backups, embeddings, vector representations, caches, logs and derived artefacts, subject to any legally required retention and to the backup retention arrangements set out below. Where Company Materials are held in secure, encrypted backup or archive media from which targeted deletion is not technically practicable, the Supplier may retain such copies until expiry of its standard backup retention cycle, which shall not exceed ninety (90) days from the relevant trigger event. During that period the Supplier shall isolate and protect such copies in accordance with paragraphs 10.3 and 10.4, shall not access, restore, use or process them for any purpose, and shall securely destroy them on expiry of that cycle. Where Company Materials are retained under a legal requirement, the Supplier shall isolate and protect them in accordance with paragraphs 10.3 and 10.4 and delete them on expiry of the retention period. The Supplier shall provide written certification, signed by an authorised representative, confirming completion of the deletion and cessation of processing required by this paragraph. Where any copies are retained under the backup retention carve-out above or under a legal requirement, the certification shall identify those copies, the basis for retention and the date of scheduled destruction, and the Supplier shall provide a further certification confirming destruction within ten (10) business days of that date.

11. Information Security Incidents and Breaches

11.1 The Supplier shall create, operate, maintain, review, improve and test, at least annually, a Security Incident Management Plan.

11.2 The Supplier shall record, classify, investigate, manage and remediate any Information Security Incident (including any AI Incident and any personal data breach) or Information Security Breach in accordance with this Policy and the Supplier's Security Incident Management Plan.

11.3 The Supplier shall promptly notify the Company of any actual or potential Information Security Breach affecting, or reasonably likely to affect, Company Materials, the Company's Systems Environment, or the Goods and/or Services. Such notification shall be without undue delay and in any event no later than twenty-four (24) hours after the Supplier becomes aware of the actual or potential Information Security Breach and shall be submitted through the following notification channels:

a) Company's Privacy and Resilience, by email to privacy@centrica.com and resilience@centrica.com;
b) Company's Global Operations Centre, by phone on +44 (0) 1753 494500 and by email to GSOC@centrica.com;
c) Where relating to a Personal Data Breach:
    i. in the UK, by e-mail to both privacy@centrica.com and resilience@centrica.com and by telephone to the Global Operations Centre +44 (0)1753 494 500);
    ii. in Ireland, by e-mail to both dataprotection@bordgais.ie and resilience@centrica.com and by telephone to the Global Operations Centre +44 (0)1753 494 500);
    iii. in both the UK and Ireland, by notifying the contacts specified in both paragraphs (c) and (d); and
d) Any other incident management, security escalation or notification channels agreed between the parties for the purposes of the Agreement.

11.4 Initial notification shall include, to the extent known, the nature of the incident, affected services, affected Company Materials, affected systems, initial containment actions, likely impact, point of contact and next update cadence.

11.5 The Supplier shall provide regular updates throughout investigation and remediation of any Information Security Breach (and any related Information Security Incident), including containment actions, root cause analysis, impact assessment, corrective actions, recovery status, lessons learned and closure evidence in accordance with the Company's applicable security, data protection, privacy, and incident management plans.

11.6 The Supplier shall preserve evidence, logs, records and affected environments as required to support investigation, forensic analysis, regulatory engagement, customer-impact assessment and Company assurance.

11.7 For any material Information Security Breach, the Supplier shall perform or support computer forensic investigation in accordance with Good Security Practice and provide the Company with relevant reports, subject to legal and contractual confidentiality constraints.

11.8 The Supplier shall not unreasonably refuse any Company request to collaborate in resolving, investigating, reporting or remediating an Information Security Incident or Information Security Breach.

11.9 Information Security Incidents and Information Security Breaches shall be treated as Confidential Information.

11.10 Any unauthorised AI training on, or disclosure of Company Materials to, an AI System, generation of unlawful or harmful Outputs, or failure of an AI governance control shall constitute an AI Incident and an Information Security Incident and shall be recorded, notified to the Company without undue delay,

investigated and managed in accordance with this Section 11. Where material, such an event shall also constitute a material Information Security Breach.

12. PCI DSS

12.1 This section applies where the Supplier performs payment card transactions, collects, stores, processes, transmits or facilitates Payment Card Data, or provides any PCI In Scope Services that the Company depends on to achieve or maintain compliance with PCI DSS.

12.2 Where the Supplier provides PCI In Scope Services, the Supplier warrants and represents that it shall obtain and maintain, for the duration of the Agreement, valid PCI DSS Attestations of Compliance covering all PCI In Scope Services provided under the Agreement. Such Attestations of Compliance shall be issued by, or where applicable countersigned by, a PCI QSA. Any alternative assurance arrangement shall require prior written approval by the Company through its authorised governance route.

12.3 The Supplier shall identify whether it acts as a merchant, service provider, payment facilitator or other relevant PCI role and shall maintain a responsibility matrix identifying the respective PCI DSS responsibilities of the Supplier and the Company.

12.4 The Supplier shall restrict access to Payment Card Data, details of PCI In Scope Services and related PCI environments to Supplier Personnel and Subcontractors who require such access to perform approved obligations under the Agreement.

12.5 The Supplier acknowledges that it is responsible for the security of Payment Card Data to the extent that the Supplier, Supplier Personnel or Subcontractors could directly or indirectly impact the security of Payment Card Data or the Company's PCI DSS compliance. The Supplier shall maintain segmentation, access control, logging, encryption, vulnerability management, secure development and other controls applicable to the PCI scope in accordance with Good Security Practice, PCI DSS and this Policy.

12.6 The Supplier shall promptly notify the Company of any change to PCI scope, PCI evidence, service provider status, payment flow, payment processor, segmentation control, control environment, Subcontractor involvement or PCI In Scope Services that may affect Company obligations, PCI DSS compliance or risk.

13. Operational Technology Security

13.1 This section applies where the Supplier provides Goods and/or Services that are classed as, connect to, support, monitor, operate, maintain or may otherwise affect Operational Technology or essential operational functions.

13.2 The Supplier shall comply with Good Security Practice, applicable industry standards, regulations and guidance for securing OT, including IEC 62443 where applicable.

13.3 The Supplier shall maintain OT governance, risk management, asset management, secure architecture, Supplier management, monitoring, incident response and lifecycle controls proportionate to the criticality and safety impact of the OT service.

13.4 The Supplier shall implement defence-in-depth controls appropriate to the criticality of the OT environment, including network zoning and segregation, least privilege access, multi-factor authentication, secure remote access, system hardening, malware protection, secure configuration management, network

monitoring, backup and recovery controls, and segregation between Operational Technology and Information Technology environments.

13.5 The Supplier shall maintain an accurate and complete inventory of OT assets, systems, software, firmware, interfaces, network connections and critical dependencies used in connection with the Goods and/or Services and shall review the inventory at least annually and following Material Change.

13.6 The Supplier shall conduct OT-specific cyber security risk assessments, including threat modelling where appropriate, before implementation of new OT solutions and following Material Change. The Supplier shall document identified risks, compensating controls and remediation actions and make such evidence available to the Company on request.

13.7 The Supplier shall implement capabilities to detect, monitor and investigate cyber security events affecting OT environments, including logging, alerting, anomaly detection and retention of security records sufficient to support incident response, forensic investigation and regulatory requirements. The Company may request evidence of such monitoring arrangements.

13.8 The Supplier shall maintain and test incident response, business continuity and disaster recovery arrangements for OT Goods and/or Services. Such arrangements shall include restoration procedures, backup and recovery capabilities, resilience measures, lessons learned processes and escalation arrangements proportionate to the operational and safety impact of the service.

13.9 The Supplier shall ensure that all hardware, software, firmware and services used within the OT environment are obtained from trusted sources and subjected to appropriate supply-chain assurance activities. The Supplier shall provide evidence of vulnerability management, independent security testing, remediation activities and security assurance of critical suppliers on request.

13.10 The Supplier shall ensure that any remote access to OT environments is authorised, monitored, encrypted, protected by multi-factor authentication and restricted to approved personnel operating under least privilege principles. Remote access shall be disabled when no longer required and shall not bypass established security controls.

13.11 The Supplier shall ensure that changes affecting OT environments are risk assessed, tested, authorised and implemented through a documented change management process. Changes that may affect safety, resilience or security shall be subject to enhanced review and approval prior to implementation.

14. Vulnerability and Patch Management

14.1 The Supplier shall maintain vulnerability and patch management processes covering Software, infrastructure, Cloud Services, APIs, endpoints, operating systems, databases, network devices, AI Technology and any third-party components used in connection with the Goods and/or Services. The patch management requirements set out in paragraph 14.2 apply to supplier-released security patches from the date such patches become available. The vulnerability remediation requirements set out in paragraph 14.11 apply to vulnerabilities identified through vulnerability scanning, penetration testing or other assurance activities, where remediation may require patching, configuration changes, code remediation, architectural changes, compensating controls or other risk treatment measures. Where AI Technology or Cloud Services are operated by a third party and the Supplier is not able to apply security patches directly, the Supplier shall monitor the provider's security advisories and patch status, apply all updates and configuration changes available to it within the timelines in paragraph 14.2, escalate material delays to the provider, and notify the Company promptly on becoming aware that a vulnerability affecting the Goods and/or Services will not be,

or has not been, remediated within the applicable timeline in paragraph 14.2, and in any event within twenty-four (24) hours of the expiry of that timeline, and implement compensating controls pending remediation.

14.2 Security patches shall be applied from the date of supplier release within the following mandatory timelines unless a Company-approved Control Exception applies:

(a) Urgent or actively exploited vulnerabilities: appropriate mitigating or compensating controls shall be implemented within twenty-four (24) hours, and the relevant security patch shall be applied within forty-eight (48) hours;
(b) Critical vulnerabilities (CVSS 9.0–10.0): appropriate mitigating or compensating controls shall be implemented within forty-eight (48) hours, and the relevant security patch shall be applied within seven (7) calendar days;
(c) High vulnerabilities (CVSS 7.0–8.9): the relevant security patch shall be applied within fourteen (14) calendar days;
(d) Medium vulnerabilities (CVSS 4.0–6.9): the relevant security patch shall be applied within thirty (30) days;
(e) Low vulnerabilities (CVSS 0.1–3.9): the relevant security patch shall be applied within one hundred and twenty (120) calendar days.

Any mitigating or compensating controls implemented in respect of Urgent or actively exploited vulnerabilities or Critical vulnerabilities shall remain in place until the relevant security patch has been successfully applied and its effectiveness validated. The implementation of mitigating or compensating controls shall not extend the applicable patching timeline unless approved by the Company through a Control Exception.

14.3 The Supplier shall manage vulnerable, unsupported, end-of-life or end-of-support software components in accordance with Section 16 (Software Supply Chain Security) and the vulnerability remediation requirements of this Section.

14.4 Unsupported, end-of-life or end-of-support components shall not be used unless approved compensating controls are implemented, documented in the Risk Register and accepted through a Control Exception.

14.5 The Supplier shall use appropriate vulnerability detection and dependency monitoring processes, including Software Composition Analysis where applicable, to identify vulnerable components and remediate findings in accordance with the required timelines.

14.6 The Supplier shall record and report unsuccessful or overdue patching where a patch was not installed within the required period, repeatedly failed, or was not applied due to approved or pending exception.

14.7 Where the Supplier's Systems Environment is connected to the internet, the Company's Systems Environment or other organisations/networks, the Supplier shall perform vulnerability scanning at least monthly and upon any Material Change that may affect information security.

14.8 The Supplier shall perform penetration testing at least annually and upon Material Changes that may affect information security, service risk or Company Materials. The Supplier shall produce a report of the findings of each vulnerability scan and penetration test (a "**Test Report**").

14.9 Vulnerabilities identified by scanning or penetration testing shall be assigned severity using an industry-recognised scoring methodology including CVSS v3.1 or later where applicable.

14.10 The Supplier shall identify vulnerabilities as "**Urgent Priority**" where they are actively exploited, affect internet-facing systems, permit unauthenticated remote code execution, impact payment card data, special category personal data, Business-Critical Services, OT, SCADA or are confirmed as exploited within Supplier or Company environments.

14.11 Vulnerabilities identified through vulnerability scanning, penetration testing or other assurance activities shall be mitigated and remediated within the following mandatory timelines, calculated from the date on which the Supplier first identified, or ought reasonably to have identified, the vulnerability, unless a Company-approved Control Exception applies:

(a) **Urgent Priority:** appropriate mitigating or compensating controls shall be implemented within twenty-four (24) hours, and the vulnerability shall be fully remediated within forty-eight (48) hours;
(b) **Critical:** appropriate mitigating or compensating controls shall be implemented within forty-eight (48) hours, and the vulnerability shall be fully remediated within seven (7) calendar days;
(c) **High:** the vulnerability shall be fully remediated within fourteen (14) calendar days;
(d) **Medium:** the vulnerability shall be fully remediated within thirty (30) calendar days; and
(e) **Low:** the vulnerability shall be fully remediated within one hundred and twenty (120) calendar days.

For the purposes of this paragraph, full remediation includes applying any available security patch and implementing any configuration change, code remediation, architectural change or other permanent corrective measure necessary to remove or reduce the vulnerability to a level approved by the Company. Any mitigating or compensating controls implemented in respect of Urgent Priority or Critical vulnerabilities shall remain in place until full remediation has been completed and validated and shall not extend the applicable remediation timeline unless approved by the Company through a Control Exception.

14.12 The Supplier shall validate the effective implementation of mitigating or compensating controls and the effective remediation of vulnerabilities by subsequent scanning or, for Urgent Priority, Critical, High or Medium findings where appropriate, penetration testing, and shall produce a report of the findings of such validation (a "**Validation Test Report**"). Validation of full remediation shall be completed within the applicable final remediation timeline set out in paragraph 14.11. Where validation shows that mitigation or remediation was not effective, the vulnerability shall be treated as never having been mitigated or remediated, as applicable.

14.13 The Supplier shall provide complete and unredacted Test Reports, Validation Test Reports and consolidated remediation tracking to the Company on request. Where the request relates to an Urgent Priority finding, Information Security Incident, Information Security Breach or Regulatory Authority enquiry, the Supplier shall provide relevant evidence within forty-eight (48) hours where practicable and subject to contractual confidentiality constraints.

14.14 Where remediation timelines cannot be met for Company-impacting services, data or systems, the Supplier shall notify the Company promptly on becoming aware that the timeline will not be met, and in any event within twenty-four (24) hours of its expiry, document compensating controls, record the risk in the Risk Register and seek formal risk acceptance where required.

15. Secure Software Development

15.1 Where the Supplier or its Subcontractors develop, configure, customise or modify Software in connection with the Agreement, they shall do so in accordance with Good Security Practice and secure development requirements.

15.2 Before development commences, the Supplier shall establish secure development policies, standards, procedures, practices, test methods and quality controls.

15.3 Where Software may require installation, integration or operation within the Company's Systems Environment, the Supplier shall identify, understand and comply with relevant Company Policies, procedures and working practices.

15.4 This paragraph applies only where the Supplier or any Subcontractor provides Endpoint Software, and shall not otherwise apply. Proportionate to the nature and risk of the Endpoint Software, the Supplier shall:

(a) supply Endpoint Software either signed with a valid code-signing certificate issued by a recognised certificate authority, or distributed through an official browser or platform store, together with version and hash information where applicable, and notify the Company before any signing certificate expires or is replaced;
(b) disclose to the Company before deployment the privileges required, data collected, network domains and ports used, persistence mechanisms and update behaviour of the Endpoint Software;
(c) make updates available for deployment through the Company's software deployment and change processes, and not deliver updates that bypass those processes unless approved in writing by the Company. Any change to the privileges, data collected, network domains, persistence mechanisms or update behaviour disclosed under (b) shall be a Material Change; version updates that do not alter those matters shall not. Delay attributable to the Company's deployment processes shall not count against the timelines in paragraph 14.2, provided the Supplier made the update available and notified the Company promptly;
(d) provide reasonable cooperation, documentation and access to installation media to support any security testing of the Endpoint Software that the Company elects to carry out. The Supplier shall procure all rights and permissions necessary to enable the Company and its authorised testers to analyse, test and, to the extent permitted by applicable law, decompile the Endpoint Software solely for security assurance purposes. Any results shall be treated as Confidential Information; and
(e) ensure the Endpoint Software can be fully removed, and support its removal on termination or on the Company's request.

15.5 The Supplier shall not use Company production data in development or testing unless expressly approved in writing by the Company and protected by appropriate data protection, security and confidentiality controls.

15.6 Software shall undergo security verification appropriate to its type and risk, including OWASP ASVS Level 2 or higher for web applications/APIs, OWASP MASVS Level 2 or higher for mobile applications and documented testing against agreed security requirements for other Software.

15.7 High-risk applications, including those processing payment data, special category personal data or large volumes of user records, shall meet enhanced standards specified by the Company, such as OWASP ASVS Level 3 where applicable.

15.8 The Supplier shall integrate automated security testing into development workflows, including SAST, DAST, secret scanning, security gates and other testing appropriate to the Software and associated risks.

15.9 The Supplier shall conduct threat modelling during design and update threat models following material architectural changes. Threat models shall document identified threats, attack vectors and implemented mitigations.

15.10 The Supplier shall not deploy Software to production that contains Critical or High severity vulnerabilities unless formal risk acceptance has been approved by the Company's CSO or authorised delegate and compensating controls have been implemented and documented.

15.11 The Supplier shall maintain release, code review, configuration, segregation of environments, secrets management and change records necessary to demonstrate secure development compliance.

15.12 Any Software or code generated in whole or in part using any AI System or AI tool (including AI coding assistants) shall be subject to the same development, testing, review, approval and security assurance requirements as Software developed without such tools. The Supplier shall remain fully responsible for such Software or code, including for any Security Defect, vulnerability or third-party rights infringement arising from its use.

16. Software Supply Chain Security

16.1 The Supplier shall identify, assess and manage software supply-chain risks associated with Software, open-source components, third-party libraries, dependencies, development tools, build pipelines and third-party software providers.

16.2 The Supplier shall perform Software Composition Analysis (SCA) and dependency monitoring throughout the software lifecycle to identify vulnerable, unsupported, malicious or unauthorised components.

16.3 The Supplier shall maintain and provide on request a complete, accurate and current Software Bill of Materials (SBOM) for Software, applications, platforms, APIs and components used in connection with the Goods and/or Services. The SBOM shall identify third-party libraries, dependencies, open-source components, proprietary components, version information and support status.

16.4 The Supplier shall ensure that vulnerable, unsupported, end-of-life or unapproved software components are identified, risk assessed and remediated in accordance with the Supplier's vulnerability management process and the requirements of this Policy.

16.5 The Supplier shall ensure that relevant Subcontractors, software suppliers and component providers maintain appropriate software supply-chain assurance records and SBOMs where applicable. The Supplier shall provide evidence of such assurance on request.

16.6 The Supplier shall promptly notify the Company of any software supply-chain compromise, malicious component, dependency compromise, unauthorised code insertion or other event that may affect the security, integrity or resilience of the Goods and/or Services.

17. Secure AI Development and Operation

17.1 Where the Supplier develops, modifies, integrates, fine-tunes, configures or operates Service AI Systems pursuant to the Agreement, it shall implement the requirements of this section to the extent technically supported and proportionate to the nature, intended use and risk of the relevant Service AI System. Where a Service AI System comprises, incorporates or relies on an AI System, model or AI Technology developed, trained and supplied by a third party which the Supplier does not develop, train, fine-tune or materially modify (a "**Third-Party AI Component**"), paragraphs 17.2 to 17.5 and 17.11 shall apply: (a) in full to the configuration, integration, data pipelines, prompts, guardrails, access controls, evaluation at Output level and deployment environment within the Supplier's control; and (b) in respect of the Third-Party AI Component itself, to the extent of the documentation, controls, evaluation tooling and assurance

information made available by the third-party provider, which the Supplier shall obtain, maintain and make available to the Company. The Supplier shall disclose to the Company any material limitation in the information or controls available from the third-party provider prior to deployment. The Supplier may not rely on this paragraph where the limitation arises from its own failure to obtain reasonably available information, to enable or configure available provider controls, or to select a provider capable of supporting the requirements of this Policy.

17.2 The Supplier shall document datasets, data sources, data quality assessments, bias testing, lawful basis for processing where personal data is involved, model selection, model versioning, training configuration and evaluation results.

17.3 The Supplier shall maintain reproducible model development and training processes with version control and change records.

17.4 The Supplier shall evaluate Service AI Systems against defined metrics for accuracy, robustness, fairness, security, safety, explainability and operational performance appropriate to risk and use case.

17.5 The Supplier shall implement explainability mechanisms appropriate to the risk level and use case of each Service AI System, sufficient to enable the Company to understand the basis on which Outputs and decisions are produced.

17.6 The Supplier shall implement content provenance or marking mechanisms where a Service AI System generates or materially alters content, where technically feasible and proportionate.

17.7 The Supplier shall ensure that any legally required AI-generation disclosures, metadata, tags, indicators or watermarks embedded in Outputs remain intact and are not removed or altered without the Company's prior written approval.

17.8 The Supplier shall use non-reversible anonymisation techniques where Company Materials are approved for secondary AI development or testing purposes outside their original approved purpose.

17.9 The Supplier shall monitor Service AI Systems after deployment for drift, misuse, security threats, bias, output quality, unsafe behaviour, human oversight interventions and AI Incidents.

17.10 The Supplier shall maintain AI assurance evidence, including Service AI System inventory, risk assessments, AIBOMs, technical documentation, testing and validation results, audit reports, compliance evidence and AI Incident reports.

17.11 Where the Supplier provides, operates or relies on any Service AI System, the Supplier shall implement and maintain AI-specific security controls proportionate to the risk, including protection against prompt injection, data leakage, model inversion, model extraction, unauthorised inference-time learning, secure API management and role-based access control, and shall test the effectiveness of such controls at appropriate intervals.

18. Logging and Monitoring

18.1 For the purpose of detecting, investigating and reporting Security Defects, Information Security Incidents and Information Security Breaches, the Supplier shall create and maintain logs for security, system, administrator, user, API, application, AI, OT and relevant physical security events within the Supplier’s Systems Environment.

18.2 Logs shall be complete, accurate, protected from unauthorised access, alteration, corruption or destruction, and retained securely such that the unavailability of a system, application or Facility does not also make corresponding logs unavailable.

18.3 The Supplier shall retain logs in accordance with the Company's records retention policies and requirements, where applicable, and in compliance with the Agreement, applicable laws, regulations, and data protection obligations. In all cases, logs shall be retained for no less than six (6) months unless a longer retention period is required by the Company, applicable law, regulatory requirements, or the Agreement.

18.4 Systems shall synchronise time to an approved reliable time source where practicable. Event timestamps shall be recorded in UTC and include source, user, action, object, result and other details relevant to investigation.

18.5 At a minimum, logs shall capture authentication success and failure, account creation and deletion, privileged activity, bulk data import/export, object access/change/delete/copy/move, API authentication and authorisation decisions, input validation failures, rate limiting activations, web application security events, security control changes, deployment activity and suspicious behaviour patterns.

18.6 The Supplier shall correlate and monitor events for indications of Security Defects, Information Security Incidents, Information Security Breaches, unauthorised access, data exfiltration, control bypass, vulnerability exploitation, AI misuse, OT anomalies and unusual privileged activity.

18.7 For Service AI Systems processing Company Materials or supporting Company operations, AI logs shall include model identifier and version, input prompts and outputs where permitted and minimised, confidence scores or rationales where applicable, guardrail activations, human oversight interventions and training or fine-tuning events involving Company Materials.

18.8 Where detailed Service AI System logging, traceability or explainability functionality is not technically supported or cannot be met, the Supplier shall disclose such limitations to the Company, to the extent reasonably practicable, prior to using the relevant Service AI System, and shall cooperate to provide alternative assurances or documentation where reasonable.

18.9 Where any logs under this Section 18 contain, or may contain, personal data, the Supplier shall:

(a) provide all information and assistance reasonably required to enable the Company to carry out a data protection impact assessment under Article 35 of the UK GDPR (or equivalent) in respect of such processing, and, where such assessment identifies a high risk that has not been mitigated to the Company's reasonable satisfaction, shall not commence or continue the relevant processing pending the Company's written instructions;
(b) process such personal data only on the Company's documented instructions and in accordance with the Data Processing Schedule;
(c) apply data minimisation and, where reasonably practicable, pseudonymise, redact or anonymise the personal data contained in such logs;
(d) subject always to the minimum retention period in paragraph 18.3, retain such logs only for so long as is necessary for the purposes for which they were created and, where a log must be retained for security, audit or legal purposes beyond that period, pseudonymise or redact the personal data within it for the remainder of the retention period, and permanently delete the log and all copies, including from backups, caches, vector representations and embeddings, once that retention period expires; and

(e) ensure that its Affiliates, Subcontractors and any third-party AI provider are bound by obligations no less protective than this paragraph 18.9, and that none of them uses such logs to train, fine-tune, validate or otherwise improve any AI System or AI Technology.

18.10 The Supplier shall provide logs, log extracts and monitoring evidence promptly on Company request to support investigation, audit, assurance, regulatory engagement or incident response.

19. Physical Security

19.1 This section applies where the Supplier is responsible for physical security of Facilities, offices, data centres, contact centres, call centres, storage locations or other premises used in provision of the Goods and/or Services.

19.2 The Supplier shall comply with physical security requirements aligned to ISO 27001 or a substantially equivalent standard and shall maintain physical security policies, standards and procedures.

19.3 Facilities used to process, store or access Company Materials shall be protected using appropriate physical access controls, visitor management, secure areas, access reviews, monitoring, environmental controls and secure storage practices.

19.4 The Supplier shall apply clean desk, clear screen, confidential waste, secure printing and secure storage practices where Company Materials may be handled in physical form.

19.5 Physical security events relevant to Company Materials, the Supplier's Systems Environment or the Goods and/or Services shall be logged, monitored, investigated and reported in accordance with this Policy.

19.6 The Supplier shall undertake and maintain a documented physical security risk assessment for each Facility at which the Goods and/or Services are provided, or at which Company Materials, Company assets or Company personnel may be present. Such assessment shall be reviewed at least annually and following any Material Change affecting the physical security risk environment of the relevant Facility. The Supplier shall make the current assessment and supporting documentation available to the Company on request for review and assurance purposes, and shall record identified risks, compensating controls and remediation actions in the Risk Register maintained under paragraph 4.6.

20. Awareness and Training

20.1 The Supplier shall ensure that all Supplier Personnel complete information security and AI awareness training programmes, including relevant obligations for data protection, acceptable use, phishing, incident reporting, secure handling of Company Materials and emerging technologies such as AI.

20.2 In addition to the Supplier's own training under paragraph 20.1, where Supplier Personnel are granted access to the Company's Systems Environment, Company Materials or the Goods and/or Services, the Supplier shall ensure that such personnel complete any Company-mandated training and acknowledgements notified by the Company, in the form and at the frequency required by the Company.

20.3 Training shall be completed within thirty (30) working days of employment, before access is granted to the Company's Systems Environment, Company Materials or the Goods and/or Services, and thereafter at least annually.

20.4 The Supplier shall provide role-based training for privileged users, developers, service desk personnel, incident responders, AI users, AI developers, OT support personnel and personnel handling regulated, customer or sensitive data.

20.5 The Supplier shall maintain records of training completion and provide evidence to the Company on request.

20.6 The Supplier shall promptly revoke, suspend or deny relevant access where Supplier Personnel have not completed mandatory training or are not adequately trained for the services they perform.

21. Subcontractor Security Management

21.1 The Supplier shall ensure that its Subcontractors comply with the requirements of this Policy throughout the term of the Agreement. The Supplier shall remain fully responsible and liable for the acts, omissions, security posture, compliance and performance of its Subcontractors as if such acts, omissions, security failures, non-compliance or performance failures were those of the Supplier itself.

21.2 The Supplier shall include in Subcontractor contracts obligations that are substantially the same as, and no less onerous than, the requirements of this Policy, including assurance, security incident notification, audit support, data handling, training, confidentiality, access control, AI, OT, resilience and exit obligations where applicable. Where a Subcontractor is a provider of Cloud Services, foundation models, General-Purpose AI models (as defined by the EU AI Act) or other AI Technology supplied on standard terms which are not reasonably open to negotiation, the Supplier shall: (a) procure contractual protections as close to the requirements of this Policy as is reasonably achievable; (b) disclose to the Company the relevant terms and any material gaps against this Policy; and (c) implement compensating controls approved by the Company. This paragraph does not limit paragraph 21.1, and the Supplier shall remain fully responsible and liable for such Subcontractors.

21.3 The Supplier shall obtain Company approval or provide prior notification, as required by the Agreement or Company instruction, before engaging or materially changing Subcontractors that may access, process, store, transmit, support or impact Company Materials or the Goods and/or Services. Unless otherwise agreed in writing by the Company, such notification shall be provided not less than thirty (30) calendar days before the proposed engagement or material change. Where personal data is processed, the provisions in the data protection part of the agreement shall prevail, including any requirement to obtain the consent of the Company in relation to appointment of a sub-processor.

21.4 The Supplier shall conduct risk-based due diligence and ongoing monitoring of Subcontractors and maintain evidence of Subcontractor security compliance at least to the same level conducted by the Company of the Supplier.

21.5 The Supplier shall maintain records of risk-based due diligence, ongoing monitoring and security assurance activities for Subcontractors and shall provide such information to the Company on request. Where reasonably required by the Company, the Supplier shall provide assurance evidence relating to relevant Subcontractors through the Company's approved supply-chain assurance platform (currently Risk Ledger) to support supply-chain security, risk assessment and nth-party assurance activities.

21.6 The Supplier shall investigate Subcontractor compliance at a frequency determined by risk assessment and at least once during the term of the relevant Subcontractor arrangement, or more frequently where reasonably requested by the Company.

21.7 The Supplier shall ensure that Subcontractors do not process Company Materials outside the locations set out for them in the Location Statement, or otherwise approved under paragraph 6.7, or outside approved systems, purposes or contractual arrangements.

22. Business Continuity, Disaster Recovery and Operational Resilience

22.1 The Supplier shall maintain, test and evidence business continuity, disaster recovery and operational resilience arrangements proportionate to the criticality of the Goods and/or Services and sufficient to support the Company's continuity and operational resilience requirements for the Goods and/or Services as notified to the Supplier.

22.2 Such arrangements shall include continuity plans, recovery objectives, backup, restoration and rebuild processes, incident escalation, dependency mapping, key personnel arrangements, technology dependencies, Facilities, Subcontractors, Cloud Services, critical Suppliers and service restoration priorities. The Supplier shall maintain such arrangements and supporting documentation as are necessary to support the Company's continuity planning and resilience assessments.

22.3 The Supplier shall test business continuity and disaster recovery arrangements at least annually and following Material Change, and at such greater frequency as is appropriate to the criticality of the Goods and/or Services. The Supplier shall provide the Company with evidence of test completion, results and outcomes sufficient to demonstrate that its arrangements remain capable of supporting the Company's continuity and recovery requirements.

22.4 The Supplier shall record test outcomes, issues, lessons learned, corrective actions and improvement plans, including remediation timelines for any material risk or deficiency identified, and provide evidence to the Company within ten (10) business days of such request, including where reasonably required to support the Company's resilience governance, assurance or regulatory obligations.

22.5 For Business-Critical Services, the Supplier shall promptly, and in any event, within twenty-four (24) hours of becoming aware, notify the Company of resilience events, continuity plan invocation, material service degradation, failed resilience tests, unsupported dependencies or other matters that may affect continuity of the Goods and/or Services, or that may adversely affect the Company's ability to execute its business continuity and operational resilience plans.

22.6 The Supplier shall ensure backup and restoration arrangements protect Company Materials and support recovery in accordance with agreed service, regulatory and security requirements and the Company’s recovery objectives.

22.7 Where a Service AI System is material to the delivery or operation of the Goods and/or Services, the Supplier shall maintain appropriate contingency and transition arrangements (forming part of its ISMS and business continuity arrangements) to ensure continuity in the event that such Service AI System becomes unavailable, or is suspended, withdrawn or materially restricted. The Supplier shall notify the Company without undue delay, and in any event, within twenty-four (24) hours, where a foundation model provider, AI hosting provider or other material AI provider ceases support for, materially restricts or withdraws any Service AI System, model family or capability used in connection with the Goods and/or Services, and shall promptly, and in any event, within five (5) business days, propose mitigating measures, which may include deployment of an equivalent alternative Service AI System subject to the Company's prior written approval (not to be unreasonably withheld or delayed) and applicable change control.

22.8 The Supplier shall identify to the Company each Material Subcontractor supporting the Goods and/or Services, shall keep that identification current, and shall ensure that each Material Subcontractor

maintains continuity, recovery and resilience capabilities and contractual obligations sufficient to support the requirements of this Section 22. The Supplier shall maintain contingency arrangements for the failure or unavailability of any Material Subcontractor. The Company may, acting reasonably, designate a Subcontractor as a Material Subcontractor, and the Supplier shall treat it as such from the date notified. Notification of any proposed change to a Material Subcontractor shall be given in accordance with paragraph 21.3. This paragraph is without prejudice to paragraph 21.1.

23. Governance, Records, Reporting and Audit

23.1 The Supplier shall provide information security records and reports required by this Policy, the Agreement or Company request to the Company's CSO or authorised delegate.

23.2 The Supplier shall maintain a record covering each non-compliance with this Policy, including description, risk, root cause, owner, remediation plan, target date, compensating controls, approval status and closure evidence (the "**Non-Compliance Record**").

23.3 Non-compliance shall be recorded promptly following discovery and reported to the Company as required by the Agreement, annually and on request.

23.4 The Supplier shall maintain evidence sufficient to demonstrate compliance with this Policy, including policies, standards, procedures, risk assessments, treatment plans, registers, training records, audits, certification, vulnerability reports, incident records, logs, AI evidence, OT evidence, continuity evidence and Subcontractor assurance evidence.

23.5 In relation to Service AI Systems, audits may include the Supplier's governance, controls, testing, validation, compliance processes and records relating to such Service AI Systems, including the Supplier's obligations relating to Company Materials, Outputs and Training Data under the Agreement. The Supplier shall maintain documentation sufficient to demonstrate compliance with its obligations relating to Service AI Systems, including inventories, data flows, Training Data categories, logging practices, testing records, risk assessments, approval records, Training Data provenance records and governance documentation. The Company may use any information and documentation provided under this paragraph for audit, regulatory and third-party assurance purposes, subject to appropriate confidentiality protections. Nothing in this paragraph requires the Supplier to disclose source code, model weights or model parameters, and the Company shall disclose information provided under this paragraph to third parties only where those third parties are bound by confidentiality obligations no less protective than those in the Agreement.

23.6 The Company or its nominated Auditor may audit the Supplier's compliance with this Policy in accordance with the Agreement, including inspection of records, interviews with Supplier Personnel and inspection of Supplier premises or systems where appropriate.

23.7 Audits shall be conducted remotely where appropriate and shall be subject to reasonable notice. Except where the audit relates to suspected fraud, breach, Information Security Breach, Regulatory Authority request or other circumstances where notice is not appropriate or permitted, the Company shall endeavour to provide not less than five (5) business days' written notice of the audit.

23.8 The Supplier shall perform a risk-based security audit of the Supplier's Systems Environment annually and upon Material Change. The Supplier shall provide audit reports, findings and remediation plans to the Company on request.

23.9 The purpose of audit includes assurance of compliance, investigation of complaints or queries, provision of information required by a Regulatory Authority or customers, investigation of suspected fraud or wrongful practice, and support for Company financial reporting audits where applicable.

23.10 The Supplier shall cooperate with the Auditor and provide reasonable access and assistance needed to exercise audit rights, while minimising unnecessary disruption to service delivery where practicable.

23.11 The Supplier shall report risk acceptances, Policy exceptions, overdue remediation, audit findings, incidents, material changes, Subcontractor issues and control failures to the Company where such matters may affect Company Materials, Company systems, service delivery, compliance or risk.

24. Control Exceptions, Risk Acceptance and Material Change

24.1 Where the Supplier is unable to meet any requirement of this Policy, the Supplier shall document the non-compliance, associated risk, compensating controls, remediation plan, target date and accountable owner.

24.2 No deviation from this Policy shall be deemed accepted unless formally approved in writing by the Company through an authorised governance route.

24.3 The Supplier shall track all approved Control Exceptions to closure and provide status reporting to the Company on request.

24.4 The Supplier shall notify the Company in advance of any Material Change that may affect security, resilience, compliance, location, data processing, Subcontractor support, architecture, hosting model, the use or operation of any Service AI System, access arrangements, connectivity, service operation or control environment of the Goods and/or Services.

24.5 The Company may require additional assurance, due diligence, risk assessment, audit, testing, remediation evidence, reassessment activities, contractual update or approval before a Material Change is implemented. The Company may also require such activities following an Information Security Incident, Information Security Breach or AI Incident, or where there is a material change to the Supplier's risk profile, ownership, control, financial standing, use of Subcontractors, hosting arrangements, security posture, compliance status or use of Service AI Systems, where reasonably necessary to assess Information Risk associated with the Goods and/or Services.

24.6 The Supplier shall not implement a Material Change that materially increases Information Risk to the Company without prior engagement with the Company and completion of required assurance or approval activities.

25. Insurance

25.1 The Supplier shall maintain appropriate insurance cover, taking into account the nature of the Goods and/or Services provided and the risks arising from its performance of the Agreement. Such cover shall, where relevant, provide protection in respect of public liability, employers' liability, professional indemnity, cyber liability and data breach risks.

25.2 Where the Supplier processes, stores, transmits or otherwise has access to Company Materials, the Supplier shall maintain insurance appropriate to the information security and data protection risks associated with the Services. Such cover shall, where relevant, provide protection against risks including data breaches, network security incidents, cyber extortion or ransomware events, privacy liabilities,

incident response costs, regulatory investigations and defence costs (where insurable), business interruption arising from cyber, network security or data-related incidents, intellectual property liabilities, media liabilities and liabilities arising from the Supplier's use of AI Systems or AI Technology in connection with the Goods and/or Services.

25.3 The Supplier shall provide reasonable evidence of insurance cover upon request and at each renewal of the cover, and shall notify the Company of any material reduction, cancellation or non-renewal of such cover.

25.4 For the avoidance of doubt, nothing in this section limits any insurance requirements set out elsewhere in the Agreement.