TERMS AND CONDITIONS OF PURCHASE

The purchase of products or services ("Products") by China Telecom (Europe) Limited and its divisions, subsidiaries, and affiliates ("CTE" or "Ordering Party") are subject to these terms and conditions ("Agreement") regardless of other or additional terms or conditions that conflict with or contradict this Agreement in any purchase order, non-negotiated document, quote, acknowledgement, or other communication. Pre-printed terms and conditions on any document of supplier ("Providing Party") and/or CTE's failure to object to conflicting or additional terms will not change or add to the terms of this Agreement. If the parties have a negotiated agreement for the relevant Products, such terms will govern and supersede these terms and conditions.

1. **PURCHASE ORDERS.**
   Any order placed by CTE will be made with CTE's standard purchase order form and submitted in writing by fax, or electronic means acceptable to CTE ("Purchase Order"). Providing Party shall acknowledge CTE's Purchase Orders in writing within one (1) business day of receipt. Purchase Order acknowledgments shall contain Providing Party's promised delivery date ("Delivery Date"). Furthermore, any partial fulfilment of a Purchase Order will be deemed accepted by Providing Party.

   CTE may cancel any Purchase Order having a clerical error within five (5) business days of placing such Purchase Order. CTE may change or cancel Purchase Orders or reschedule Delivery Date for any Products ordered, provided that it notifies Providing Party at least ten (10) business days prior to the latest confirmed Delivery Date. Providing Party shall not modify or substitute any part of a Purchase Order without CTE's prior written consent. CTE may cancel a Purchase Order without liability at any time if Providing Party breaches any term of this Agreement or fails to deliver within the agreed time.

   In the event of any conflict between the terms and conditions set out in any parts of the Agreement, the terms shall be applied in the following order in decreasing order of precedence: (a) the special terms agreed in the Purchase Order; (b) the terms and conditions of this Agreement and its Schedule and Annexes; (c) the Service Level Agreement; and (d) any other document incorporated by express reference.

2. **APPOINTMENT.**
   Providing Party authorizes CTE to distribute or resell Products purchased under this Agreement worldwide through its Affiliates or through third party representatives appointed by CTE. Providing Party shall not restrict CTE's or its Affiliate's' rights to market, distribute, or sublicense the Products under CTE's brand or under Providing Party's branding, as CTE may determine. "Affiliate" shall mean any person, partnership, joint venture, company, corporation or other form of enterprise, domestic or foreign, that directly or indirectly controls or owns, is controlled or owned by, or is under common control or ownership with CTE.

3. **PRICES.**
   The price for any Products will be set forth in CTE's Purchase Order. CTE shall not be liable for taxes with respect to any Purchase Order other than any sales tax which Providing Party is required by law to collect from CTE.

   A. PRICE PROTECTION.
      In the event that Providing Party decreases the price of any Product, CTE will be entitled to a credit equal to the difference between the net price paid by CTE, less any prior credits granted by Providing Party, and the new decreased price for the Product multiplied by the quantity of such Product in CTE's inventory or in transit on the effective date of the reduction.

i. CTE shall submit to Providing Party, not later than sixty (60) business days after receiving notice of such price decrease, a Product inventory report as of the effective date, together with a debit memo reflecting the credit described above.

ii. Providing Party shall be deemed to have verified the Product inventory report and debit memo unless Providing Party contests the same in writing within sixty (60) business days after receiving such report and memo.

iii. Uncontested debit memos shall be credited to CTE's account as of the effective date of such price decrease.

B. PRODUCTS SHIPPED AFTER PRICE DECREASE.
Products shipped on or after the effective date of any price decrease will be shipped and invoiced at the price in effect at the time of shipment.

C. PRODUCTS SHIPPED AFTER PRICE INCREASE.
Products shipped after the effective date of any price increase will be shipped and invoiced at the price in effect at the time of Purchase Order placement.

4. TERMS OF PAYMENT.

The invoice shall only be issued after the receipt of Acceptance Certificate from CTE against Clause 5 DELIVERY AND TITLE and Clause 6 ACCEPTANCE AND PRODUCT RETURN. Payment terms for Products purchased in CTE's Purchase Order shall be net sixty (60) calendar days from date of invoice. CTE will also receive an additional 2% discount if payments are made within 10 calendar days of the invoice date. CTE has the right of offset against Providing Party for programs, promotions, special pricing, rebates, and for any CTE returns as described herein. Incorrect invoices shall be returned for correction and shall not be payable until corrected and reissued.

5. DELIVERY AND TITLE.

All Products will be delivered DDP CTE's destination (Incoterms 2020) as stated in CTE's Purchase Order. Providing Party agrees to deliver Products ordered by CTE to the location and within the Delivery Date specified in CTE's Purchase Order pursuant to the terms of this Agreement.

Providing Party may not ship before the promised shipment date ("Shipment Date") without CTE's prior written approval. The Providing Party shall ship the Equipment no later than the Shipment Date, as evidenced by the on-board date stated on the original bill of lading. Timely shipment or delivery is of the essence for delivery of Products. If the Providing Party fails to ship or delivery the Equipment within the Ship Date or Delivery Date, CTE shall be entitled, without prejudice to any other remedies, to claim liquidated damages in the amount of 10 % of the relevant Purchase Order per day of delay, up to a maximum of 100%. If the delay exceeds ten (10) days, CTE shall have the right to terminate the relevant Purchase Order in whole or in part.

Providing Party agrees to pay premium freight when its delivery will miss the acknowledged Delivery Date. CTE may designate the carrier to be used, and, in absence of such specification by CTE, Providing Party shall select a carrier in its reasonable discretion.

Providing Party warrants the title to all Products sold to CTE and warrants that such Products are not subject to security interests, liens, or other encumbrances. Title and risk of loss shall pass upon the receipt of Acceptance Certificate from CTE against Clause 6 ACCEPTANCE AND PRODUCT RETURN. For the avoidance of any doubt, under no circumstance shall CTE be the importer of record for this engagement. Providing Party shall remain fully responsible for all import duties, customs formalities, and associated liabilities.

6. ACCEPTANCE AND PRODUCT RETURN.

All Products are subject to inspection and testing prior to acceptance, in accordance with any specific acceptance standards or requirements agreed in the Purchase Order or any other written documents. In the absence of any such agreed standards or requirements, the Products shall be delivered in accordance with CTE's satisfactory standards. CTE will use reasonable efforts to give Providing Party notice of any obvious defects, damage, or discrepancy. Acceptance shall be deemed only upon written confirmation in the form of a signed acceptance certificate ("Acceptance Certificate") issued by CTE following full inspection.

Acceptance will not be deemed a waiver of any warranty hereunder or otherwise provided by law. If CTE finds that the Products or any part thereof do not conform to the requirements of the Purchase Order, Providing Party will, at CTE's election either: replace such nonconforming Products, accept return for credit at the invoice price, or refund CTE's purchase price for such nonconforming Products.

Discovery of latent defects or nonconformities shall be subject to return at Providing Party's cost at any time within the applicable warranty period. Return of Products that are not in conformance with the Purchase Order (including DOA), over- shipments, recalled products, and shipments rejected due to early or late delivery will be returned freight collect at Providing Party's risk and expense.

7. DEFECTIVE PRODUCT.

Notwithstanding any other provision of this Agreement, CTE may return for full credit of CTE's cost of the Product (including, without limitation, cost of assembling, disassembling, transportation, and labour), less any prior credits issued by Providing Party, any and all Products found to be defective upon delivery, or within a reasonable time thereafter; provided, however, that any such defective Products are returned to Providing Party, freight collect, within ninety (90) business days of CTE's discovery of the defect.

8. END OF LIFE.

If Providing Party discontinues Products or makes Products obsolete, Providing Party shall notify CTE at least ninety (90) business days prior to the effective date of such change. CTE will then notify Providing Party of the affected Products in its inventory for Providing Party's repurchase. All end of life Products will be subject to the return policy in Section 6 ACCEPTANCE AND PRODUCT RETURN. Furthermore, the Providing Party will grant CTE the right of a lifetime buy upon request.

9. WARRANTY

A. COMPLIANCE WITH LAW.

Providing Party guarantees CTE that the design, construction and quality of the Products shall comply in all respects with all requirements of any statutory regulation, order, contract (including the Regulatory Compliance Schedule of these Terms and Conditions of Purchase) or any other instrument having the force of law, which may be in operation at the time when the Products are supplied.

B. PROVIDING PARTY'S MANUFACTURER'S WARRANTY.

Providing Party warrants the Products in accordance with the greater of the following: (i) the manufacturer's standard warranty, (ii) the warranty that is publicly posted on manufacturer's website, (iii) the warranty that is required by local law, or (iv) 24 months for those purchases originating from Asia or the European Union. CTE is authorized to pass this warranty through to CTE's customers and to end users. The warranty period as set forth in this Section 9 WARRANTY shall begin to run with respect to CTE's customers and any end user upon delivery of the Product to the end user. Any Product to be returned under the terms of the warranty may be shipped to Providing Party either from CTE or directly from CTE's customers or end users. Providing Party shall indemnify CTE for any liability related to a breach of warranty.

C. NEW/UNUSED PRODUCT.
Providing Party warrants that the Products provided to CTE by the Providing Party are new and unused.

D. PRODUCT CONFORMANCE TO MANUFACTURER'S SPECIFICATIONS.
Delivery of any Product by Providing Party to CTE shall constitute a warranty by Providing Party that the Product conforms to the manufacturer's specifications.

Warranty terms shall apply globally, irrespective of the Product's delivery destination or end-user location. In the event of a warranty breach, CTE may require, at its sole discretion, refund, repair, or replacement of defective Products, plus all related costs including removal, reinstallation, and logistics.

10. ORIGINAL MANUFACTURE PARTS.

Providing Party represents and warrants that it is either the original equipment manufacturer ("OEM"), original component manufacturer ("OCM"), or a franchised or authorized distributor of the OEM/OCM for the Products; or if Providing Party is not the OEM/OCM or a franchised or authorized distributor of the OEM/OCM, then Providing Party confirms by acceptance of Purchase Orders hereunder that the Products have been procured from the OEM/OCM or a franchised or authorized distributor of the OEM/OCM.

11. SERVICES PERFORMED.

Providing Party shall provide Services in accordance with the Purchase Order and related document as agreed between Providing Party and CTE. Services in this Agreement shall include but not limited to installation, testing, maintenance and all other services agreed in the Purchase Order. Where applicable, any Providing Party's equipment located on CTE's site remains at all times the risk of the Providing Party, which shall insure such equipment against all risk of loss or damage. CTE accepts no liability for any loss of or damage to Providing Party's equipment, however caused, including through CTE's negligence. Providing Party shall perform all services with the highest degree of professional skill and care in accordance with industry best practices. Providing Party shall not subcontract services without CTE's prior written consent.

12. INTELLECTUAL PROPERTY

A. PROVIDING PARTY INTELLECTUAL PROPERTY WARRANTY.
Providing Party warrants that any and all Product purchased hereunder, and the manufacture, sale, or use thereof, do not and will not violate or infringe upon any patent, copyright, trademark, trade secret, or other intellectual property right of any third party.

B. INDEMNIFICATION.
Providing Party will indemnify, defend, and hold CTE, its successors, assigns, customers and end-users harmless against all losses, damages, costs and expenses (including reasonable attorneys' fees and costs of establishing rights to indemnification and any settlement) based on any claims, demands, suits, proceedings and actions ("Claim") in connection with any alleged infringement of any patent, copyright, trademark, trade secret or other intellectual property right of a third party, including any Claims that the Product, or the process, design, or methodology used to manufacture the Product, infringes any third party patent, copyright, trademark, trade secret or other intellectual property rights.

C. CTE'S OBLIGATION WITH RESPECT TO PROVIDING PARTY'S IP INDEMNITY.
CTE will provide Providing Party with written notice of any such Claims, grant full authority to Providing Party to defend and settle such Claims, and upon Providing Party's request, provide reasonable assistance and information, at Providing Party's cost and expense.

D. PROVIDING PARTY'S OBLIGATION IN EVENT OF IP CLAIM. If a Product becomes the subject of a Claim or CTE is enjoined from selling or using a Product, Providing Party will:

i. procure for CTE the right to sell and use the Product;

ii. provide CTE with replacement or modified Product that is non-infringing; or

iii. if Providing Party is unable to provide the remedies above, refund the full purchase price for such Product.

13. GENERAL INDEMNIFICATION.

Providing Party will indemnify, defend and hold CTE harmless of and from any and all liabilities, losses and damages (including costs, expenses and attorneys' fees, and costs of establishing rights to indemnification) resulting from any claim of any CTE's customers or any third party (including employees of CTE or Providing Party), for any claim including: (a) death or personal injury; (b) breach by Providing Party of any warranty, representation, or covenant under this Agreement; (c) breach of contract; (d) non-compliance with requirements hereunder or applicable laws, regulations, directives, or ordinances; or (e) damage to property arising out of, or in any way connected with, the Products or the sales, distribution, use or operation thereof. This indemnity shall also cover breaches of data protection obligations (including GDPR), cybersecurity incidents, and any regulatory investigations or penalties imposed on CTE due to Providing Party's actions or omissions.

14. LIMITATION OF LIABILITY.

CTE WILL NOT BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY NATURE ARISING OUT OF OR RELATED TO THE PURCHASE PURCHASE ORDERS OR ANY TERMINATION, REJECTION, OR REVOCATION OF ACCEPTANCE OF THE PURCHASE ORDERS, INCLUDING WITHOUT LIMITATION, BUSINESS INTERRUPTION COSTS, REPROCUREMENT COSTS, LOSS OF PROFIT OR REVENUE, PROMOTIONAL OR MANUFACTURING EXPENSES, OVERHEAD, INJURY TO THE REPUTATION OF PROVIDING PARTY, OR LOSS OF CUSTOMERS, EVEN IF CTE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL CTE'S LIABIITY EXCEED THE PRICE SET FORTH IN THE PURCHASE ORDER.

15. USE OF TRADEMARKS/TRADENAMES.

CTE is authorized to use Providing Party's trademarks, trade names and logos in connection with CTE's sale of Products. CTE will have the right to pass on this right of usage to its reseller customers.

16. CONFIDENTIALITY.

If either party receives from the other party written information marked "Confidential" and/or "Proprietary", the receiving party agrees not to use such information except in the performance of this Agreement, and to treat such information in the same manner as it treats its own confidential information. The obligation to keep information confidential shall not apply to any such information that has been disclosed in publicly available sources; is, through no fault of the party receiving the confidential information, disclosed in a publicly available source; is in the rightful possession of the party receiving the confidential information without an obligation of confidentiality; or is required to be disclosed by operation of law. Except as otherwise provided herein, the obligation not to disclose shall be for a period of five (5) year after the disclosure of the Confidential Information. Any breach of this clause shall entitle CTE to seek injunctive relief, specific performance, or other equitable remedies, in addition to damages.

17. EXPORT.

Providing Party acknowledges and agrees that CTE may export Products as allowed by the export control laws, regulations and orders of the United States and other countries to which it may ship Products. The parties shall observe and comply with all applicable laws, rules and regulations applicable to the performance of their respective obligations under this Agreement including, but not limited to, anti-corruption laws (such as the U.S. Foreign Corrupt Practices Act) and regulations in respect of import or export of Products.

18. GLOBAL SUPPLY CHAIN SECURITY COMPLIANCE.

Providing Party warrants and represents to CTE as follows: (1) if eligible for Customs-Trade Partnership Against Terrorism ("C-TPAT"), or other comparable customs certification programs, Providing Party will be certified and validated and Providing Party will provide CTE with its Status Verification Interface ("SVI") number(s), or other program identification information, to confirm the foregoing representation prior to shipment; (2) if not eligible for C-TPAT, or other comparable customs certification programs, Providing Party fully understands the requirements for C-TPAT certification and will make all commercially reasonable efforts to comply to this certification program and assist CTE with maintaining its certification with this compliance request. Providing Party will provide evidence of such compliance, including security certifications and results of internal security audits as CTE may reasonably require; (3) if Providing Party's status under this Subsection changes, Providing Party will give prompt written notice to CTE; and (4) Providing Party will comply with any pre- arranged visit CTE's auditors may make to verify if Providing Party's procedures are in accordance with the criteria set forth by C-TPAT or other comparable customs compliance program. The obligations in this clause are ongoing and shall survive termination of the contractual relationship, to the extent necessary to ensure compliance with relevant supply chain security frameworks and regulatory obligations.

19. STATUTORY CONFORMANCE.

With respect to the Products ordered under this Agreement, Providing Party warrants and agrees that it has complied with all applicable federal, state and local laws, codes and requirements. Providing Party especially warrants that all Products supplied to CTE comply with all applicable laws in the EU and transposed directives into national laws in the member states, e.g. environmental legislation such as substance regulation RoHS / REACH, technical conformity CE and waste management. Providing Party shall undertake to comply and bear all costs for the compliance with the current and applicable EU legislation. Providing Party agrees to indemnify and hold harmless CTE, its successors and assigns, and the customers of any of them, from all loss, damages, costs and expenses (including reasonable attorneys' fees and costs of establishing rights to indemnification) which may be incurred by non-compliance of Providing Party with this paragraph. CTE reserves the right to return any non-compliant Product at the expense of Providing Party.

20. OZONE DEPLETING SUBSTANCES.

CTE reserves the right to reject any Products containing or manufactured with substances identified as a Class I or Class II ozone depleting substances by the U.S. Environmental Protection Agency pursuant to Title VI of the Clean Air Act Amendments of 1990, and any amendments thereto, whether or not such Products shall be required to bear labelling.

21. CTE AUDIT RIGHTS.

Providing Party shall maintain complete, accurate, and up-to-date records relating to its performance under this Agreement, including compliance with applicable laws, regulations, and the requirements set forth herein. Providing Party agrees to the following:

A. CTE and its authorised representatives shall have the right, upon reasonable advance notice and during regular business hours, to access Providing Party's facilities, systems, and records, including those of any subcontractors, for the purpose of auditing compliance with this Agreement;

B. Providing Party shall provide CTE with copies of, or access to, all relevant books, documents, certifications, records, data, and other materials as may be reasonably requested by CTE to verify such compliance;
C. Providing Party shall cooperate fully with CTE's audit efforts and shall not unreasonably delay or obstruct any audit or request for documentation; and
D. This audit right shall survive termination or expiration of this Agreement for a period of three (3) years, or longer if required by applicable law.

22. SANCTIONS AND EXPORT CONTROL COMPLIANCE.

Providing Party warrants and represents to CTE as follows:

E. Providing Party is not designated on, owned or controlled by, or acting for any person or entity designated on, any sanctions or restricted parties list administered by the European Union, United States (including the U.S. Office of Foreign Assets Control), United Nations, United Kingdom, or other applicable authority;
F. Providing Party is not incorporated in or operating from any jurisdiction that is subject to comprehensive sanctions or embargoes, including without limitation Cuba, Iran, North Korea, Syria, or the Crimea, Donetsk, or Luhansk regions of Ukraine, unless expressly authorised under applicable law;
G. The goods, software, and technology supplied under this Agreement do not originate from, contain components from, or transit through any sanctioned country, region, or party unless explicitly authorised by relevant authorities;
H. Providing Party shall comply with all applicable export control and sanctions laws and regulations, including those of the European Union, United States, United Kingdom, and other relevant jurisdictions; and
I. Providing Party shall promptly notify CTE in writing if it becomes subject to any sanctions or if any of its goods or services become subject to sanctions or export restrictions.

Any breach of this Section shall be deemed a material breach of the Agreement, entitling CTE to terminate the Agreement with immediate effect and without liability. Providing Party shall indemnify, defend, and hold harmless CTE and its affiliates, directors, officers, employees, and agents from and against any and all claims, losses, liabilities, damages, costs, and expenses (including reasonable legal fees and costs) arising out of or relating to any breach by Providing Party of its obligations under this Section 20, including any violation of applicable sanctions or export control laws and regulations. This indemnity obligation shall survive the termination or expiration of this Agreement.

23. GENERAL

A. This Agreement shall be governed, construed, and enforced in accordance with the laws of the country where the CTE entity that placed the Purchase Order ("Governing Country") is located. The courts of the Governing Country shall have jurisdiction and venue over all controversies arising out of, or relating to, this Agreement. The United Nations Convention for the International Sale of Goods shall not apply.
B. Providing Party may not assign this Agreement without the prior written consent of CTE, and CTE's affiliates may perform CTE's obligations under this Agreement. This Agreement is binding on successors and assigns.
C. This Agreement can only be modified in writing signed by authorized representatives of both CTE and Providing Party.
D. CTE and Providing Party are independent contractors and agree that this Agreement does not establish a joint venture, agency relationship, or partnership.
E. CTE's failure to object to any document, communication, or act of Providing Party will not be deemed a waiver of any of these terms and conditions. Notwithstanding any other

remedies provided in this Agreement, CTE retains all rights existing at law or equity, and CTE's failure to affect cover does not bar it from any other remedy.

F. The unenforceability of any of these terms or conditions will not affect the remainder of the terms or conditions.

G. CTE is not liable for failure to fulfil its obligations under this Agreement due to causes beyond its reasonable control (for example: acts of nature, acts or omissions of the Providing Party, operational disruptions, man-made or natural disasters, epidemic medical crises, strikes, criminal acts, delays in delivery or transportation, or inability to obtain labour or materials through its regular sources).

H. Products, including software or other intellectual property, are subject to any applicable rights of third parties, such as patents, copyrights and/or user licenses, and Providing Party will comply with such rights.

I. Providing Party and CTE will comply with applicable laws and regulations. Providing Party shall collect, process, and transfer all personal data in connection with this Agreement in accordance with the applicable privacy laws and regulations.

REGULATORY COMPLIANCE SCHEDULE

Statement of Applicability

A. Together with the terms of the Agreement between the Parties, this Regulatory Compliance Schedule excluding Annex 2 (DORA Compliance – Flow Down Obligations) shall apply in the event that the Providing Party is a "third party supplier" as defined in regulation 7(2) of Electronic Communications (Security Measures) Regulations 2022 of 1 October 2022 as amended or replaced from time to time, who supplies, provides or makes available goods, services or facilities for use in connection with Ordering Party's network or service.

B. If the end user of the Services is or becomes an EU Finance Entity as defined in article 2 of Regulation (EU) 2022/2554 of 14 December 2022 as amended or replaced from time to time, Annex 2 of this Schedule (DORA Compliance – Flow Down Obligations) shall apply. Should this Schedule (Regulatory Compliance) apply only in the scope of its Annex 2 (DORA Compliance – Flow Down Obligations), all references therein to this Schedule (Regulatory Compliance) remain valid and the referenced paragraphs of this Schedule (Regulatory Compliance) will apply accordingly.

Electronic Communications (Security Measures) Regulations 2022

China Telecom is a public electronic communications network provider and public electronic communications service provider, which means it must comply with the Communications Act 2003 (the "Act"), the Electronic Communications (Security Measures) Regulations 2022 (the "Regulations") and the Telecommunications Security Code of Practice issued pursuant to the Act ("Code of Practice").

The Regulations require China Telecom to take measures to identify and reduce the risks of security compromises occurring in relation to its network or service as a result of things done or omitted by third party suppliers. A "third party supplier" is any person who supplies, provides or makes available goods, services or facilities for use in connection with China Telecom's network or service including you, the Providing Party.

The measures that China Telecom must take include ensuring that third party suppliers comply with specific contractual terms, including those in regulation 7 of the Regulations and section 3 (Technical guidance measures) of the Code of Practice.

This Schedule (excluding Annex 2 (DORA Compliance – Flow Down Obligations) sets out the terms the Providing Party is required to comply with to enable China Telecom to comply with its obligations under the Telecoms Legislation.

UNLESS THE PARTIES AGREE OTHERWISE IN WRITING, REFERRING TO SPECIFIC PROVISIONS OF THIS SCHEDULE, OR UNLESS THE PROVISIONS OF THE AGREEMENT ARE MORE FAVOURABLE FOR THE CUSTOMER, IN THE EVENT OF A CONFLICT THIS SCHEDULE SHALL PREVAIL OVER ANY OTHER PROVISIONS OF THE AGREEMENT, ITS OTHER ADDENDA AND ORDERS.

TERMS NOT DEFINED IN THIS SCHEDULE SHALL HAVE THE MEANING ASCRIBED TO THEM IN THE AGREEMENT OR ANY AMENDMENT THERETO (AS APPLICABLE).

BACKGROUND

(A) The Ordering Party is a network provider and a service provider and, accordingly, is required to comply with laws applicable to such providers, including the Telecoms Legislation.

(B) Pursuant to regulation 7 of the Regulations, a network provider or service provider must (amongst other things) take such measures as are appropriate and proportionate to identify and reduce the risks of security compromises occurring in relation to its public electronic communications network or public electronic communications service as a result of things done or omitted by third party suppliers. Such measures include ensuring that third party suppliers comply with specific contractual terms, including those in regulation 7(4) of the Regulations and section 3 (Technical guidance measures) of the Code of Practice.

(C) The Providing Party is a third party supplier (as defined in regulation 7(2) of the Regulations).

(D) This Schedule sets out certain terms required to comply with the Telecoms Legislation.

DEFINITIONS AND INTERPRETATION

1.1 In **this Schedule**:

1.1.1 **"Act"** means the Communications Act 2003 (as amended or supplemented from time to time).

1.1.2 **"Annex"** means an annex to this Schedule, unless otherwise stated.

1.1.3 **"Code of Practice"** means the Telecommunications Security Code of Practice issued pursuant to sections 105E and 105F of the Act (as amended or supplemented from time to time).

1.1.4 **"Disaster"** is defined in paragraph 3.1.2 of this Schedule.

1.1.5 **"electronic communications network"** is defined in s. 32(1) of the Act.

1.1.6 **"electronic communications service"** is defined in s. 32(2) of the Act.

1.1.7 **"equipment"** includes both software and hardware.

1.1.8 **"Exit Period"** means each period nominated by the Ordering Party in writing which (a) commences from the receipt of the termination notice from Ordering Party or Providing Party; and (b) continue for no longer than 6 months after the receipt of the termination notice, subject to Ordering Party's discretion to extend the period.

1.1.9 **"Exit Plan"** is defined in paragraph 10.2 of this Schedule.

1.1.10 **"Exit Services"** means the services, functions and responsibilities assigned to the Providing Party under paragraph 10 (*Exit Assistance*) of this Schedule (and the Exit Plan).

1.1.11 **"Incident Management Process"** is defined in paragraph 3.1 of this Schedule.

1.1.12 **"Incident Management Process Tests"** is defined in paragraph 3.6 of this Schedule.

1.1.13 **"network data"** means the network identifiers, logs and documents that help to describe the network and the equipment in the network.

1.1.14 **"network equipment"** means either a software or hardware component of the Ordering Party's network that transmits or receives data or provides supporting services to components of the Ordering Party's network that transmit or receive data. It includes both virtual machines and physical hardware.

1.1.15 **"network equipment supplier"** is defined in paragraph 8.1 of this Schedule.

1.1.16 **"network provider"** means a person who provides a public electronic communications network.

1.1.17 **"Network Security Tests"** is defined in paragraph 5.1.1 of this Schedule.

1.1.18 **"Ordering Party Security Tests"** is defined in paragraph 5.1.2 of this Schedule.

1.1.19 **"Overarching Exit Objective"** means the need to take such measures as are appropriate and proportionate to identify and reduce the risks of security compromises occurring in relation to the Ordering Party's public electronic communications network or public electronic communications service (as applicable) arising in connection with the termination or expiry of the agreement or the relevant part thereof.

1.1.20 **"Overarching Security Obligations"** is defined in paragraph 2.1 of this Schedule.

1.1.21 **"Providing Party Personnel"** means the employees, officers, agents, affiliates, consultants, contractors and sub-contractors (of any tier) of the Providing Party, and the employees, officers, agents, consultants, contractors and sub-contractors (of any tier) of any of the foregoing.

1.1.22 **"public electronic communications network"** is defined in s. 151(1) of the Act.

1.1.23 **"public electronic communications service"** is defined in s. 151(1) of the Act.

1.1.24 **"regulation"** means a regulation of the Regulations (unless otherwise stated).

1.1.25 **"Regulations"** means the Electronic Communications (Security Measures) Regulations 2022 (as amended or supplemented from time to time).

1.1.26 **"Replacement Supplies"** means any goods, services or facilities which are the same as or substantially similar to the Supplies (or any part thereof) and which the Ordering Party will or may receive from a Successor Supplier following the termination or expiry of this agreement or any part thereof.

1.1.27 **"Schedule"** means this Schedule, unless otherwise stated.

1.1.28 **"security critical function"** means, in relation to a public electronic communications network or a public electronic communications service, any function of the network or service whose operation is likely to have a material impact on the proper operation of the entire network or service or a material part of it.

1.1.29 **"security compromise"** has the meaning given to it in s. 105A(2) of the Act, provided that, for the purposes of this Schedule, it includes any of the events, circumstances or incidents listed in s. 105A(2) of the Act happening or occurring in relation to, or being suffered by, the Providing Party and/or the Providing Party Per-

sonnel that will, may or could compromise the Ordering Party's public electronic communications network and/or public electronic communications service by virtue of the Supplies and/or the relationship of the parties pursuant to this agreement.

1.1.30 **"security incident"** means an incident involving: (a) the occurrence of a security compromise; or (b) an increased risk of a security compromise occurring.

1.1.31 **"Security Tests"** means Ordering Party Security Tests and/or Network Security Tests (as the context requires).

1.1.32 **"Security Testers"** is defined in paragraph 5.1 of this Schedule.

1.1.33 **"Security Weakness"** is defined in paragraph 5.6 of this Schedule.

1.1.34 **"sensitive data"** is defined in regulation 2 of the Regulations.

1.1.35 **"service provider"** means a person who provides a public electronic communications service.

1.1.36 **"Successor Supplier"** means each provider or potential provider of the Replacement Supplies as a successor to the Providing Party, which may be the Ordering Party, an affiliate of the Ordering party or a third party.

1.1.37 **"Supplies"** means the goods, services and facilities (or any part thereof) supplied, provided or made available to the Ordering Party by or on behalf of the Providing Party pursuant to this agreement.

1.1.38 **"Telecoms Legislation"** means, collectively, the Act, the Regulations and the Code of Practice (in each case, as amended or supplemented from time to time).

1.1.39 **"third party administrator"** means any managed service provider, provider of Ordering Party group functions or external support for the Providing Party's equipment (e.g. third-line support function).

1.1.40 **"third party supplier"** means, in relation to a network provider or service provider, a person who supplies, provides or makes available goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.

1.1.41 **"Third Party Service Provider"** means any contractor, subcontractor, agent or other third party providing any goods, software or services to the Ordering Party (and includes any Successor Supplier).

1.2 Terms used but not defined in this Schedule shall (where the context requires) have the meaning given to them in the Telecoms Legislation or, where not defined in the Telecoms Legislation, be interpreted in a way which is consistent with the Telecoms Legislation.

1.3 Notwithstanding any other term of the agreement to the contrary, in the event of any conflict or inconsistency between this Schedule (including its Annexes) and any other term of this agreement, this Schedule (including its Annexes) shall prevail. The terms of this Schedule shall prevail over its Annexes.

1.4 References in this Schedule or its Annexes to paragraphs are to the paragraphs of this Schedule or the relevant Annex (as applicable), unless otherwise stated.

2. OVERARCHING SECURITY OBLIGATIONS

2.1 The Providing Party acknowledges that the Ordering Party places great emphasis on the security of its electronic communications network and electronic communications service and that the Ordering Party is required to ensure that its third party suppliers comply with certain security obligations under the Telecoms Legislation. Accordingly, notwithstanding the Providing Party's other obligations in this Schedule, the Providing Party must comply with the following obligations (the **"Overarching Security Obligations"**):

2.1.1 the Providing Party must take such measures as are appropriate and proportionate to identify and reduce the risks of security compromises occurring in relation to the Ordering Party's public electronic communications network or public electronic communications service as a result of things done or omitted by the Providing Party (to the extent such acts or omissions relate to this agreement and/or the Supplies), including risks arising:

2.1.1.1 during the formation, existence or termination of this agreement; and

2.1.1.2 from the Providing Party contracting with other persons for the supply, provision or making available of any goods, services or facilities for use in connection with the Supplies;

2.1.2 the Providing Party must:

2.1.2.1 take appropriate measures to identify the risks of security compromises occurring as a result of the Ordering Party's use of the Supplies for the purposes envisaged by this agreement, to disclose any such risks to the Ordering Party, and to reduce any such risks;

2.1.2.2 where the Providing Party is itself a network provider and is given access to the Ordering Party's network or service or to sensitive data, take appropriate measures for the purposes mentioned in section 105A(1) of the Act, in relation to goods, services or facilities supplied, provided or made available by the Providing Party to the Ordering Party, which are equivalent to the measures that the Ordering Party is required to take in relation to the Ordering Party's network or service (which must, as a minimum, be reasonable and proportionate measures and must include such measures as may be notified to the Providing Party by the Ordering Party as equivalent measures from time to time);

2.1.2.3 enable the Ordering Party to monitor all activity undertaken or arranged by the Providing Party in relation to the Ordering Party's network or service; and

2.1.2.4 co-operate with the Ordering Party in the resolution of incidents which cause or contribute to the occurrence of a security compromise in relation to the Ordering Party's network or service or of an increased risk of such a compromise occurring;

2.1.3 the Providing Party must ensure that all network connections and data sharing with the Ordering Party, or arranged by the Providing Party (in connection with this agreement), are managed securely;

2.1.4 the Providing Party must have appropriate written plans to manage the termination of, and transition from, this agreement with the Ordering Party (including the Exit Plan

in accordance with paragraph 10 (*Exit Assistance*) of this Schedule) while maintaining the security of the Supplies and (to the extent applicable to the termination of this agreement and/or the Supplies) the Ordering Party's network or service and the Supplies; and

2.1.5 the Providing Party must notify the Ordering Party promptly in writing of any failure by or on behalf of the Providing Party to comply with this Schedule (including any failure to comply with its security obligations), such notice to include sufficient detail to enable the Ordering Party to understand the nature and extent of the failure.

3. INCIDENT MANAGEMENT PROCESS

3.1 The Providing Party must at all times during the term of this agreement (including each Exit Period) maintain (in accordance with this paragraph 3) a well-defined, tested and documented written incident management process (the **"Incident Management Process"**) which:

3.1.1 prepares for the occurrence of security compromises in order to limit the adverse effect of security compromises and enables the Providing Party and the Supplies to recover from security compromises

3.1.2 details the steps, actions and procedures to be taken to ensure that the Ordering Party continues to receive the Supplies in accordance with this agreement, and any adverse impact on the Ordering Party is minimised, if any one or more events occurs which has or may have a material detrimental impact on the Providing Party's ability to provide the Supplies and/or perform its other obligations under this agreement (any such event being a "**Disaster**"),

3.1.3 provides for mutual support between the Providing Party and the Ordering Party in the resolution of security incidents; and

3.1.4 is prepared and maintained in accordance with good industry practice.

3.2 The Incident Management Process must, as a minimum, ensure that the Providing Party has means and procedures in place for:

3.2.1 promptly identifying the occurrence of any actual or potential security compromise or Disaster and assessing its severity, impact and likely cause;

3.2.2 promptly identifying any mitigating actions required as a result of the occurrence of any security compromise or Disaster;

3.2.3 dealing with the occurrence of a security compromise or Disaster in accordance with any timescales identified in the Ordering Party's own incident management processes made known to the Providing Party (and, in any case, as soon as reasonably practicable) and without creating any risk of a further security compromise or or Disaster occurring; and

3.2.4 (where applicable to the Providing Party and/or the Supplies) dealing with any unauthorised access to, or control over, security critical functions by taking action as soon as reasonably possible, and without creating any risk of a further security compromise occurring, to ensure that only authorised users have access to the network or service,

(together, the **"Response Objectives"**).

3.3 The Providing Party's current Incident Management Process has been reviewed and accepted by the Ordering Party prior to the date of this agreement.

3.4 Notwithstanding paragraph 3.3 of this Schedule, the Providing Party must ensure that, at all times, the Incident Management Process complies with the requirements of this Schedule, and, unless otherwise agreed by the parties in writing, remains consistent with the version of the Incident Management Process reviewed by the Ordering Party in accordance with paragraph 3.3 of this Schedule.

3.5 Without limiting paragraph 3.4 of this Schedule, the Providing Party must update the BCDR Plan (and any risk assessments on which it is based): (a) on a regular basis and, as a minimum, once every 12 months; and (b) within 10 days after the implementation of any material change to this agreement and/or the Supplies. Any changes to the Incident Management Process will be subject to prior review and written approval by the Ordering Party.

3.6 The Providing Party must test the Incident Management Process by performing rehearsals based on realistic security compromise and Disaster scenarios (**"Incident Management Process Tests"**). The Incident Management Process Tests must be carried out by the Providing Party on a regular basis (and, in any event, not less than once in each 12 month period during the term of this agreement) in accordance with the testing arrangements set out in the Incident Management Process Tests.

3.7 Within 10 days after the completion of each Incident Management Process Test, the Providing Party must provide the Ordering Party with a written report relating to the Incident Management Process Tests, setting out the results of the Incident Management Process Tests, any deficiencies in the Incident Management Process revealed by the Incident Management Process Test and the Providing Party's proposals for remedying such deficiencies. The Providing Party must implement any remedial measures identified in its report as soon as reasonably possible after completion of the relevant Incident Management Process Tests.

3.8 The Providing Party must, in the event of a security compromise or Disaster occurring:

3.8.1 immediately invoke the Incident Management Process;

3.8.2 immediately notify the Ordering Party, giving all available details of the security compromise or Disaster and its effect on the Supplies (and the Providing Party shall regularly update this information);

3.8.3 comply with the Response Objectives;

3.8.4 ensure that any interruption to the Supplies is avoided or, at least, minimised to the greatest extent possible;

3.8.5 co-operate with the Ordering Party in order to mitigate the impact of the security compromise or Disaster on the Ordering Party's business;

3.8.6 continue to perform any obligations which are not affected by the security compromise or the Disaster in accordance with this agreement; and

3.8.7 remedy the security compromise or the Disaster, and restore the Supplies to their normal operation, as soon as reasonably practicable.

3.9 The Providing Party must, if required by the Ordering Party:

3.9.1 participate in the testing of the Ordering Party's and/or any Third Party Service Providers' incident management processes; and

3.9.2 permit the Ordering Party and its Third Part Service Providers to participate in joint testing of the Incident Management Process with their respective incident management processes, and providing the Ordering Party with evidence of such tests and reports of such test results,

subject to the relevant Third Party Service Provider entering into reasonable confidentiality provisions.

3.10 The Providing Party's obligations in this paragraph 3 apply regardless of what caused or contributed to the security compromise or Disaster (including, if applicable, if it was caused or contributed to by a force majeure event).

3.11 The Providing Party must ensure that the business continuity and disaster recovery plans of its subcontractors are consistent with, and integrated with, the Incident Management Process.

3.12 The Providing Party must:

3.12.1 in the event of a security incident or Disaster occurring, support the Ordering Party (including providing such co-operation, information and assistance as the Ordering Party may reasonably require) in managing and resolving the security incident, including immediately invoking the Incident Management Process; and

3.12.2 promptly provide a copy of its then-current Incident Management Process to the Ordering Party on request.

3.12.3 Security incidents and issues

4. SECURITY INCIDENTS AND ISSUES

Security incidents

4.1 The Providing Party must notify the Ordering Party promptly (and in any event within 48 hours of becoming aware of the relevant security incident) of any security incident that may have caused or contributed to the occurrence of a security compromise, or where the Providing Party identifies an increased risk of such a compromise occurring, including (without limitation) incidents in the Providing Party's development network or corporate network. The Providing Party must give all available details of the security incident and the relevant circumstances as at the time of such initial notification and must provide further details thereafter in phases as such details become available to the Providing Party.

4.2 The Providing Party must provide all such support, co-operation and assistance as the Ordering Party may require to support the Ordering Party in the investigation of incidents that cause or contribute to the occurrence of a security compromise in relation to the Ordering Party, or of an increased risk of such a compromise occurring.

4.3 If a security incident occurs, the Providing Party must:

4.3.1 find and provide a written report on the root cause of the security incident within 30 days;

4.3.2 resolve the security incident (including rectifying any security failings found) as soon as possible and in any event within 30 days; and

4.3.3 without prejudice to paragraph 4.3.2 above:

4.3.3.1 work with the Ordering Party to ensure the security incident is mitigated until the security incident is resolved (including providing all such assistance, co-operation and information as the Ordering Party may reasonably require in order to mitigate the impact of the security incident on the Ordering Party's public electronic communications service and/or public electronic communications network); and

4.3.3.2 (where possible) provide temporary work-arounds or issue fixes for the security incident (including to mitigate its impact and prevent the ongoing occurrence or reoccurrence of the security incident) until such time as the security incident is permanently resolved.

4.4 In the event that the Providing Party is unable to resolve any security failings (to the Ordering Party's reasonable satisfaction) within a reasonable timeframe (and, in any case, within 30 days of the Providing Party becoming aware of the relevant security incident), the Ordering Party may, without prejudice to its other rights and remedies, terminate the agreement (or, at the Ordering Party's sole discretion, any impacted part thereof) by providing the Providing Party with written notice of termination. The agreement (or the relevant part, as applicable) will terminate on the date specified in such notice or, where no such date is specified, immediately.

4.5 The Ordering Party will have no liability to the Providing Party in relation to any termination under paragraph 4.4 of this Schedule, other than payment of the fees or charges due in respect of any notice period prior to the effective date of termination. For the avoidance of doubt, the Ordering Party will not be liable to pay any form of break fee or termination charge to the Providing Party in connection with any termination under paragraph 4.4 of this Schedule.

Security issues

4.6 The Providing Party must remediate all security issues that pose a security risk to the Ordering Party's network or service discovered within their products within a reasonable time of being notified or becoming aware of the security issue (whichever is earlier), providing regular updates on progress in the interim. This shall include all products impacted by the vulnerability, not only the product for which the vulnerability was reported. This paragraph 4.6 is without prejudice to any obligations on the Providing Party to remediate issues more quickly contained elsewhere in this agreement.

4.7 Notwithstanding anything to the contrary (including any confidentiality obligations contained elsewhere in this agreement), the parties hereby acknowledge and agree that the Ordering Party may share details of any security issues relating to or arising out of or in connection with this agreement, its network or services, the equipment, network equipment or the Supplies (including security incidents and security compromises) with any person or third party as required to support the identification and reduction of the risks of security compromises occurring in relation to the Ordering Party's public electronic communications network and/or public electronic communications service as a result of things done or omitted by the Providing Party.

Mutual assistance and co-operation

4.8 The Providing Party shall provide such co-operation, assistance and information as the Ordering Party may reasonably require in connection with a security incident relating to the Ordering Party's network, including (without limitation) in connection with the Ordering Party's obligations pursuant to s. 105A, (*Duty to take security measures*), 105C (*Duty to take*

measures in response to security compromise), 105D (*Duty to take specified measures in response to security compromise*), 105I (*Duty to take explain failure to act in accordance with code of practice*), 105J (*Duty to inform users of risk of security compromise*) and 105K ((*Duty to inform OFCOM of security compromise*).

5. SECURITY TESTING

Ordering Party Security Tests and Network Security Tests

5.1 The Ordering Party and/or its authorised representatives (including the Ordering Party's appointed third party security testers or auditors) (collectively, **"Security Testers"**) may from time to time:

5.1.1 require the Providing Party to support any security audits, assessments or testing required by the Ordering Party in relation to its network including those necessary to evaluate the security requirements in this Schedule, including testing for the purposes of identifying the risks of security compromises occurring in relation to its public electronic communications network or public electronic communications service, which may include joint or simultaneous testing, audits and/or assessments of the Ordering Party's network, services and/or security measures and the Providing Party's network, Supplies and/or security measures (**"Network Security Tests"**); and

5.1.2 carry out such additional security tests in relation to the Providing Party's network (where the Providing Party is itself a network provider), the Supplies and/or the operation of the security measures set out in this Schedule as it may (acting reasonably) deem necessary in order to:

5.1.2.1 assess the adequacy of the Providing Party's security measures;

5.1.2.2 assess the Providing Party's compliance with this Schedule;

5.1.2.3 assess the risks of security compromises occurring in connection with the Supplies; and/or

5.1.2.4 as part of, or in order to support, the carrying out of any Network Security Tests,

such tests being **"Ordering Party Security Tests"**.

5.2 Subject to paragraph 5.3 of this Schedule, the Ordering Party shall provide the Providing Party with at least ten (10) business days' notice of any Network Security Tests or Ordering Party Security Tests.

5.3 Where the Ordering Party (acting reasonably) considers that the conduct of the Network Security Tests or the Ordering Party Security Tests will have a material adverse effect on the Providing Party's ability to deliver the Supplies in accordance with this agreement:

5.3.1 the Ordering Party shall provide the Providing Party with reasonable advance notice (but, in any event, at least twenty (20) business days' notice) of the Ordering Party Security Tests;

5.3.2 the Providing Party shall, as soon as reasonably practicable (but, in any event, within ten (10) business days) after receipt of such notice from the Ordering Party, advise the Ordering Party:

5.3.2.1 whether the conduct of the Ordering Party Security Tests will, in its reasonable opinion, have a material adverse effect on the Providing Party's ability to deliver the Supplies in accordance with this agreement; and

5.3.2.2 if so, any activities that the Providing Party and/or the Ordering Party may reasonably be able to undertake to mitigate such effect on the Supplies;

5.3.3 the Ordering Party shall, within ten (10) business days after receipt of such notice from the Providing Party, confirm in writing to the Providing Party the extent of any relief to be granted to the Providing Party in the event of any actual non-performance by the Providing Party of its obligations under this agreement as a result of the conduct of the Network Security Tests or Ordering Party Security Tests (and taking account of any mitigation activities notified by the Providing Party under paragraph 5.3.2.2 of this Schedule);

5.3.4 if there is any dispute between the parties in relation to the matters contemplated by this paragraph 5.3, the parties shall promptly escalate the matter for resolution in accordance with the dispute resolution procedure in the agreement, provided that such referral shall not (unless otherwise agreed by the Ordering Party in writing) prevent or delay the conduct of the Network Security Tests or Ordering Party Security Tests.

5.4 The Ordering Party shall notify the Providing Party of the results of the Ordering Party Security Tests and (if and to the extent required in order for the Providing Party to be able to comply with its obligations in the remainder of this paragraph 5) the relevant parts of the Network Security Tests as soon as reasonably practicable after completion of the relevant Security Tests.

Conduct of Security Testing

5.5 The Providing Party:

5.5.1 must:

5.5.1.1 provide all such support, assistance, co-operation and information as the Security Testers may reasonably require in connection with the Network Security Tests and the Ordering Party Security Tests;

5.5.1.2 ensure, so far as is possible, that the Security Tests (to the extent they are within the Providing Party's control) involve simulating techniques that might be expected to be used by a person seeking to cause a security compromise; and

5.5.2 acknowledges and agrees that any third party testing in relation to the security of network equipment can only be accepted as evidence by the Ordering Party (for the purposes of the Code of Practice) if it is repeatable, performed independently of the Providing Party and is clearly applicable to the Ordering Party's deployment (e.g. relates to the hardware, software and configuration that is being supplied) and, accordingly, that it will co-operate with the Ordering Party to ensure that any Network Security Tests and Ordering Party Security Tests are, conducted in a manner which can be accepted as evidence by the Ordering Party (which may include the use of third party Security Testers).

Security Weaknesses

5.6 Where any Security Tests reveal any:

5.6.1 actual or potential risks of security compromises occurring in relation to the Ordering Party's network or services as a result of any failures or weaknesses in the Supplies;

5.6.2 any other failure or weakness in the Supplies; or

5.6.3 any failure by the Providing Party to comply with any of the security requirements and/or its security obligations in this Schedule,

(each a "**Security Weakness**"), then, subject to paragraph 5.7 of this Schedule, the Providing Party shall notify the Ordering Party of any changes to the Supplies, and any other steps, which the Providing Party (acting reasonably) proposes to implement in order to address the relevant Security Weakness (and a proposed timetable for the implementation of such matters).

5.7 Where any Security Weakness relates to an actual or potential risk of security compromises occurring in relation to the Ordering Party's network or services that is not due to (i) any failure or weakness in the Supplies or (ii) any failure by the Providing Party to comply with any of the security requirements and/or its security obligations in this Schedule, then the Providing Party shall notify the Ordering Party of:

5.7.1 any steps which the Providing Party could itself implement in order to address the relevant Security Weakness (and the likely costs and a proposed timetable regarding the implementation of such steps); and/or

5.7.2 where known to the Providing Party (having given the matter reasonable consideration), any steps which may need to be implemented by the Ordering Party and/or the relevant Third Party Service Providers in order to address the Security Weakness.

5.8 The Providing Party's notice under paragraph 5.6 or 5.7 (as applicable) of this Schedule shall be provided to the Ordering Party as soon as possible and, in any event, within five (5) business days after notification by the Ordering Party of the results of the Ordering Party Security Tests and/or Network Security Tests under paragraph 5.4 of this Schedule, or such other period as may be agreed by the parties in writing.

5.9 Within ten (10) business days (or such other period as may be agreed in writing by the parties) after receipt of the Providing Party's proposal under paragraph 5.6 or 5.7 (as applicable) of this Schedule or any amended proposal under this paragraph 5.9, the Ordering Party shall notify the Providing Party as to whether the proposal is approved. The Ordering Party's approval shall not be unreasonably withheld, provided that the Ordering Party shall be entitled to reject the Providing Party's proposal if (in the reasonable opinion of the Ordering Party):

5.9.1 the proposal (including the proposed timetable) would be inappropriate or insufficient to address the relevant Security Weakness;

5.9.2 any proposed changes would be inconsistent with the requirements of this Schedule; and/or

5.9.3 any proposed changes would or may, in the reasonable opinion of the Ordering Party, result in the risks of security compromises occurring in relation to the Ordering Party's network or service,

in which case the Providing Party shall amend the proposal to address the Ordering Party's comments and resubmit it for approval by the Ordering Party in accordance with this paragraph 5.9.

5.10 If there is any dispute between the parties in relation to the matters contemplated by paragraph 5.9 of this Schedule, either party may refer the dispute to the dispute resolution procedure in the agreement. Until such time as the dispute is resolved in accordance with the dispute resolution procedure, the Providing Party shall comply with any additional or alternative security measures notified by the Ordering Party which are (in the reasonable opinion of the Ordering Party) necessary to address relevant Security Weakness.

5.11 Subject to the approval of the Ordering Party under paragraph 5.9 of this Schedule, the Providing Party shall implement the relevant proposal and take any other agreed steps to address the relevant Security Weakness in accordance with the approved timetable.

5.12 The Ordering Party shall notify the Providing Party promptly once the proposal is approved in principle, in which case, the proposal shall be fully agreed and implemented by the parties in accordance with the applicable contract variation provisions in the agreement (and the Providing Party shall not withhold or delay its consent to such variation).

5.13 In relation to any proposal of the Providing Party under paragraph 5.7.2 of this Schedule, the Ordering Party shall consider and take such steps as it may deem necessary to address the relevant Security Weakness.

6. USE OF DATA

6.1 For the purposes of this paragraph 6, references to **"data"** and **"information"** include both user data and network data (unless the context otherwise requires).

6.2 The Providing Party must, in relation to any information made accessible to the Providing Party by or on behalf of the Ordering Party in connection with this agreement:

6.2.1 comply with (and ensure that Providing Party Personnel comply with) the security measures in Annex 1 (*Security Measures*), as such policies may be amended, updated or supplemented by the Ordering Party from time to time by giving notice to the Providing Party, ; and

6.2.2 limit access to any such information by Providing Party Personnel and third parties to the minimum access required to provide the Supplies.

6.3 The Providing Party must (and must ensure that any third party to whom network data or user data is made available by the Providing Party must):

6.3.1 protect any network data and user data in accordance with this Schedule and any other provisions relating to the protection or security of data contained in this agreement (including Annex 1 (*Security Measures*) and provisions relating to confidentiality and personal data);

6.3.2 have controls in place to ensure that network data and user data is only visible or accessible to appropriate employees and from appropriate locations;

6.3.3 provide such co-operation, information and assistance as the Ordering Party may reasonably require to verify that its data is properly protected in accordance with this agreement, including permitting the Ordering Party to carry out audits in accordance with paragraph 9 (*Record Keeping and Audit*) of this Schedule for the purposes of such verification.

6.4 The Providing Party must only share user data and network data with the Ordering Party (and with any third parties where permitted to do so by, and in accordance with, this agreement) via an encrypted and authenticated channel.

7. THIRD PARTY ADMINISTRATORS

7.1 This paragraph 7 applies to third party administrators. The Providing Party must:

7.1.1 comply with this paragraph 7 if it is a third party administrator; and

7.1.2 ensure that any third party engaged by the Providing Party in connection with the supply, provision or making available of the Supplies which is itself a third party administrator (including any person providing external support for the Providing Party's equipment, e.g. third-line support function) complies with this paragraph 7 as if it were the Providing Party.

7.2 The Providing Party must:

7.2.1 comply with the security measures in Annex 1 (*Security Measures*) and such additional security measures as may be notified to the Providing Party from time to time; and

7.2.2 without prejudice to paragraph 7.2.1 above, at all times when the Providing Party has access to the Ordering Party's electronic communications network or service or to sensitive data, apply controls that are at least as rigorous as the Ordering Party which shall include:

7.2.2.1 any controls identified in Annex 1 (*Security Measures*); and

7.2.2.2 such other controls as may be notified to the Providing Party by the Ordering Party from time to time.

7.3 The Providing Party acknowledges and agrees that the Ordering Party shall have the right to control the Providing Party's Personnel involved in the provision of the third party administrator services ("**Administration Personnel**") and the Providing Party must ensure that the Administration Personnel comply with the Ordering Party's instructions from time to time.

7.4 The Ordering Party may at any time require the Providing Party to: (i) immediately remove any member of the Administration Personnel from the provision of the third party administrator services; and/or (ii) ensure that any member of the Administration Personnel no longer has access to the network at any time. Where any Administration Personnel are removed under this paragraph 7.4, if requested by the Ordering Party, the Providing Party must supply (at its own cost) replacement Administration Personnel. Any exercise by the Ordering Party of its rights under this paragraph 7.4 will not relieve the Providing Party of its obligations to provide the Supplies in accordance with this agreement.

7.5 The Providing Party must comply with any reasonable staff vetting and related requirements (including fit and proper checks) requested by the Ordering Party from time to time (provided such vetting, requirements and checks are compliant with applicable law).

7.6 The Providing Party must implement:

7.6.1 technical controls to prevent one provider or their network from adversely affecting any other provider or their network;

7.6.2 logical separation within the Providing Party's network to segregate customer data and networks;

7.6.3 separation between the Providing Party's management environments used for different provider networks;

7.6.4 and enforce security enforcing functions at the boundary between the Providing Party's network and the Ordering Party's network;

7.6.5 technical controls to limit the potential for users or systems to negatively impact more than one provider;

7.6.6 logically-independent privileged access workstations per network provider and service provider; and

7.6.7 independent administrative domains and accounts per provider.

7.7 The Providing Party must:

7.7.1 monitor (on an ongoing basis) and regularly audit the activities of the Administration Personnel and staff when accessing the Ordering Party's network; and

7.7.2 maintain and retain detailed, accurate and up-to-date logs relating to the security of the Providing Party's network and, to the extent that such logs relate to access into the Ordering Party's network,provide copies of such logs (in such format as the Ordering Party may reasonably require) to the Ordering Party at least once in each 12 month period and at such other times as the Ordering Party may reasonably require.

7.8 The Providing Party must ensure that the Providing Party's networks that could impact the Ordering Party undergo the same level of testing as the Ordering Party applies to its own networks (e.g. TBEST testing as set for the Ordering Party by Ofcom from time to time) including any testing notified to the Providing Party by the Ordering Party from time to time (including any testing required pursuant to paragraph 6 of this Schedule).

8. NETWORK EQUIPMENT SUPPLIERS

8.1 This paragraph 8 applies to the Providing Party if it supplies, provides or makes available network equipment to the Ordering Party (including hardware or software), i.e. it is a **"network equipment supplier"**.

8.2 This Providing Party:

8.2.1 must share with the Ordering Party a security declaration (in such format as the Ordering Party may reasonably require) at least once in each 12 month period (to be provided by such date as required by the Ordering Party), and at such other times as the Ordering Party may reasonably require, on how the Providing Party produces secure equipment and ensures its security throughout its lifetime (a **"Security Declaration"**) which:

8.2.1.1 covers all of the aspects described in (and is consistent with the approach in) Annex B (*Vendor Security Assessment*) of the Code of Practice; and

8.2.1.2 identifies any differences in processes across product lines;

8.2.1.3 is signed-off by the Providing Party at an appropriate governance level;

8.2.2 is encouraged to openly publish its Security Declaration; and

8.2.3 where the Providing Party claims to have obtained any internationally recognised security assessments or certifications of their equipment (such as Common Criteria or NESAS), whether in a Security Declaration or otherwise, the Providing Party must share with the Ordering Party the full findings that evidence this assessment or certificate promptly following the Ordering Party's request; and

8.2.4 adhere to a standard no lower than the Providing Party's most-recent Security Declaration.

8.3 The Providing Party must (on an ongoing basis) provide the Ordering Party with up-to-date guidance (in such format as the Ordering Party may reasonably require from time to time) on how the Providing Party's equipment should be securely deployed. Such guidance must be clear, legible and sufficiently detailed to allow a reasonable skilled technical person to safely and securely deploy the equipment in accordance with the guidance.

8.4 The Providing Party must support all equipment (including all software and hardware components thereof) for the duration of the applicable period of support specified in this agreement.

8.5 The Providing Party must maintain complete, accurate and detailed records (including products and versions) of all major third party components and dependencies, including open source components and the period and level of support, relating to the equipment and the Supplies (**"Network Equipment Details"**) and provide a copy of such Network Equipment Details to the Ordering Party at least once in each 12 month period (at such time as the Ordering Party may reasonably require) and at such other times promptly following the Ordering Party's request.

8.6 The Providing Party must:

8.6.1 provide critical security patches for equipment to the Ordering Party separately to feature releases where this would maximise the speed at which the patch can be deployed; and

8.6.2 provide such critical security patches to the Ordering Party as soon as they become available (unless otherwise agreed between the parties in writing).

8.7 The Providing Party must:

8.7.1 maintain, and comply with, a vulnerability disclosure policy which is prepared in accordance with good industry practice and which must include, as a minimum, a public point of contact and details around timescales for communication; and

8.7.2 provide a copy of its then-current policy to the Ordering Party on request.

9. RECORD KEEPING AND AUDIT

9.1 The Providing Party must:

9.1.1 support any security audits, assessments or testing required by the Ordering Party in relation to the security of the Ordering Party's own network including those necessary to evaluate the security requirements in this Schedule; and

9.1.2 give to (or procure the giving to) the Ordering Party, its auditors and authorised third party agents (together, the **"Ordering Party Auditors"**) reasonable access to the Providing Party's premises, resources, personnel, systems, records and other relevant materials (and those of its subcontractors in connection with the provision of the Supplies and/or the performance of the agreement in relation to the Ordering Party's network or service) at such times as the Ordering Party may require, subject to reasonable prior written notice to the Providing Party indicating the scope of the proposed audit, for the purposes of auditing the security of the Ordering Party's own network and/or the security requirements in this Schedule (including the Providing Party's compliance with such requirements),

and the Providing Party must provide all such co-operation, assistance and information as the Ordering Party and/or any Ordering Party Auditor may reasonably require in connection with this paragraph 9.1.

9.2 Without prejudice to the Ordering Party's other rights or remedies, if any audit or assessment under this paragraph 9 reveals any failure by the Providing Party to comply with its obligations under this Schedule, the Providing Party must promptly rectify such failure as soon as reasonably practicable and at its own cost.

10. EXIT ASSISTANCE

General

10.1 The Providing Party must, during each Exit Period, co-operate with the Ordering Party and (where applicable) each Successor Supplier to ensure the orderly migration from the Supplies to the Replacement Supplies, having regard to the Overarching Exit Objective.

Preparation of Exit Plan

10.2 Within 60 days of the date of this agreement, the Providing Party must prepare a draft exit plan which sets out (in relation to the transfer of the whole or any part of the Supplies from the Providing Party to the Successor Supplier):

10.2.1 the activities required to be undertaken by the Providing Party, the Ordering Party and the Successor Supplier to ensure a timely and orderly transfer of the Supplies from the Providing Party to the Successor Supplier, and the relevant timetable; and

10.2.2 any specific measures required by the Ordering Party to give effect to the Overarching Exit Objective in connection with the transfer (including any specific data and/or information security measures),

(the **"Exit Plan"**) and submit that plan to the Ordering Party for its review and written approval.

10.3 The Providing Party must prepare draft updates to the Exit Plan from time to time to ensure that it is up-to-date and accurately reflects the then current version of the Supplies, the manner of their provision and any measures required to give effect to the Overarching Exit Objective in connection with the transfer of the Supplies. Such updates will be prepared by the

Providing Party and submitted to the Ordering Party for its review at least annually and also: (a) within 30 days after the implementation of any material change to this agreement and/or the Supplies (including following the addition or removal of any new goods, services or facilities); (b) within 5 days after the date of any notice of termination of the agreement (or any part thereof); and (c) at least 90 days prior to the expiry of the agreement (or any part thereof). Any changes to the Exit Plan under this paragraph 10.3 will be subject to the written approval of the Ordering Party.

10.4 The Providing Party shall, following the Ordering Party's review of the Exit Plan submitted pursuant to paragraph 10.2 or 10.3 above, amend the Exit Plan as reasonably required by the Ordering Party until the Exit Plan is approved in writing by the Ordering Party.

Exit obligations

10.5 During each Exit Period, the Providing Party must: (a) comply with its obligations under this paragraph 10 and the Exit Plan (in accordance with good industry practice and in such a manner so as to cause as little disruption as possible to the businesses and operations of the Ordering Party): and (b) provide all reasonable information, assistance and co-operation and appropriate resources to the Ordering Party and any Successor Supplier to facilitate the orderly transfer to the Successor Supplier in accordance with the Exit Plan and the Overarching Exit Objective.

10.6 Except as otherwise agreed between the parties in the Exit Plan, the Providing Party will provide the Exit Services at no additional charge or cost to the Ordering Party during the Exit Period and, thereafter, at rates accepted and pre-approved by the Ordering Party in writing.

10.7 The Ordering Party may terminate each Exit Period at any time by giving not less than 5 days' written notice to the Providing Party.

10.8 Without prejudice paragraph 10.5 of this Schedule, the Ordering Party may, at any time before or on expiry or termination of this agreement or the Supplies (or, in each case, any part thereof) for any reason, at the ordering Party's sole discretion, require the Providing Party to continue to provide the Supplies (or any part thereof), on the same terms (including the charges), for a maximum period of 12 months after the date on which the agreement or the Supplies (or, in each case, the relevant part thereof) would have otherwise terminated or expired.

assignment and subcontracting

10.9 Notwithstanding anything to the contrary, the Providing Party must not assign, novate, subcontract or otherwise transfer any of its obligations under this agreement (in whole or part) without the prior written consent of the Ordering Party.

10.10 Unless otherwise agreed in writing between the parties, the Providing Party must ensure that each subcontractor complies with this Schedule.

10.11 The Providing Party is responsible and liable for the acts and omissions of its subcontractors as if they were the Providing Party's acts and omissions.

Annex 1 – Security Measures

1. GENERAL SECURITY OBLIGATIONS

1.1 The Providing Party must take such measures as are appropriate and proportionate for the purposes of:

1.1.1 identifying the risks of security compromises occurring;

1.1.2 reducing the risks of security compromises occurring; and

1.1.3 preparing for the occurrence of security compromises.

1.2 The Providing Party must remove or change default passwords and accounts for all devices in the network and should disable unencrypted management protocols. Where unencrypted management protocols cannot be disabled, the Providing Party must limit and mitigate the use of these protocols as far as possible.

1.3 The Providing Party shall ensure that all security-relevant logging is enabled on all network equipment and sent to the applicable network logging systems.

1.4 The Providing Party must ensure that equipment is in a secure-by-default configuration, based on the principle that only required services are made available.

1.5 The Providing Party must prioritise critical security patches over functionality upgrades wherever possible.

1.6 The Providing Party must deploy all security related patches and patches with a security element in a way that is proportionate to the risk of security compromise that the patch is intended to address (as outlined in Table 2 (*Criticality and exposure-adjusted maximum timeframes for application of patches (from supplier release date)*) in the Code of Practice). Should this not be possible, patches shall be deployed as soon as practicable and effective alternative mitigations put in place until the relevant patch has been deployed. Where a patch addresses an exposed, actively-exploited vulnerability, the Providing Party shall ensure that such patches are deployed as soon as can reasonably be achieved, and at most within 14 days of release.

1.7 The Providing Party must have in place and maintain appropriate security measures, in accordance with best industry practice, to protect the Ordering Party's network or service and prevent security compromises occurring (to the extent relevant to the Supplies). Examples include:

1.7.1 Encryption of data in the database;

1.7.2 Encryption of hard disks / storage;

1.7.3 Encryption of data during transport;

1.7.4 Physical access controls;

1.7.5 Doors and locks, and the protection of premises by means such as alarms, security lighting or CCTV;

1.7.6 Physical separation of assets;

1.7.7 Access controls;

1.7.8 Privilege and identity management;

1.7.9 Two-factor authentication;

1.7.10 No default passwords;

1.7.11 PEN testing;

1.7.12 Pseudonymisation, anonymisation and hashing;

1.7.13 Asset disposal.

Annex 2 – DORA Compliance – Flow Down Obligations

China Telecom may be an ICT third party service provider under Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, as amended or replaced from time to time ("DORA") when providing its services to financial entities referred to in Article 2 paragraph 2 of DORA ("Financial Entities").

Financial Entities are obliged to impose certain mandatory contractual obligations on China Telecom acting as an ICT third-party service provider, and indirectly on its subcontractors (ICT subcontractors under DORA). This Annex 2 sets out the terms under which China Telecom flows-down the DORA related obligations to the Providing Party and its further subcontractors.

This Annex is aimed at allowing China Telecom's customers being Financial Entities (as defined in paragraph 1 below) to meet their regulatory requirements under DORA.

Except as expressly specified otherwise in this Annex or other applicable contractual documentation, this Annex does not create any rights (express or implied) that the Providing Party or its Critical Subcontractors will be entitled to enforce against the Ordering Party or the Customers.

1. DEFINITIONS

1.1 The following capitalized terms used in this Annex have the meanings set out below:

1.1.1 "Annex" means this DORA Compliance Annex.

1.1.2 "**Auditor**" means the Customer, the Customer's third-party auditor or a Competent Authority, or any person appointed by them in the capacity of an auditor.

1.1.3 "**Customer**" means China Telecom's Financial Entity customer receiving ICT services incorporating Providing Party's Services as defined herein.

1.1.4 "**Competent Authority**" means any EU or EU Member State official authority, government agency or other government body having regulatory, supervisory or governmental authority over the Customer, including a resolution authority if appointed for the Customer.

1.1.5 "**Critical or important function of the Customer**" means a function whose disruption would materially impair the financial performance of the Customer, or the

soundness or continuity of its services and activities, or whose discontinued, defective or failed performance would materially impair the continuing compliance of the Customer with the conditions and obligations of its authorization, or with its other obligations under the Applicable Financial Laws.

1.1.6 "**Critical Subcontractor**" means a Providing Party's subcontractor that effectively underpins the Services supporting a Critical or important function of the Customer, or a material part thereof, including one that provides services whose disruption would impair the security or continuity of the Services supporting a Critical or important function of the Customer.

1.1.7 "**Customer**" means a Financial Entity to which the Ordering Party provides (directly or indirectly) the Services.

1.1.8 "**ICT Incident**" means an unplanned event or a series of linked events that compromises the security of the Services and has an adverse impact on the availability, authenticity, integrity or confidentiality of Customer data processed in relation to the Services.

1.1.9 "**Financial Entity**" means one of financial entities as referred to in Article 2, paragraph 2 of DORA.

1.1.10 "**Services**" means services provided by the Providing Party to the Ordering Party that qualify as ICT Services as defined in Article 3, point 21) of DORA.

2. SCOPE AND APPLICATION

2.1 This Annex supplements the Agreement and is binding between the Parties during the whole period of the Agreement.

2.2 This Annex applies only if and to the extent all the following conditions are met:

2.2.1 the Providing Party provides the Services to the Ordering Party under the Agreement,

2.2.2 The Ordering Party further provides the Services or any part of them to the Customer under a separate agreement between the Ordering Party and the Customer, irrespective of whether the Services are bundled with other the Ordering Party services provided to the Customer or whether they are independently forwarded to Customer in an "as is" format,

2.2.3 the Customer remains a Financial Entity as defined in paragraph 1.1.9,

2.2.4 the Services or any part of them, alone or bundled with the Ordering Party services, support a Critical or important function of the Customer, or material parts thereof, of which the Customer informed the Ordering Party, and such information was forwarded to the Providing Party.

3. SERVICE LEVEL, INFORMATION SECURITY AND BUSINESS CONTINUITY

3.1 In providing the Services, the Providing Party will comply with the service levels set out in the Agreement.

3.2 The Overarching Security Obligations as provided in paragraph 2 (*Overarching Security Obligations*) of *Regulatory Compliance* Schedule, the provisions on the use of data as provided in paragraph 7 (*Use of Data*) of *Regulatory Compliance* Schedule as well as the security

measures contained in Annex 1 (*Security Measures*) will apply in relation to the Services.

3.3 In addition to the Incident Management Process established under paragraph 4 of the Regulatory Schedule which will apply accordingly, the Providing Party will notify the Ordering Party of any development that could have a material impact on the Providing Party's ability to effectively provide the Services in accordance with the Agreement or applicable laws – promptly, and within no more than 48 hours of obtaining relevant information. In particular, the Providing Party will notify the Ordering Party of an ICT Incident related to the Services, and will provide the Ordering Party with reasonably requested support in relation to such ICT Incident if it impacts the Ordering Party's Customers.

3.4 To the extent it applies to the Services, the Providing Party will ensure that the Providing Party Personnel and each Critical Subcontractor (including any cloud infrastructure provider that is a Critical Subcontractor) are subject to confidentiality, security and data privacy requirements that are at least as protective as the terms included in the Agreement and this Annex.

3.5 The Parties agree that the Ordering Party can disclose the information provided by the Providing Party under this paragraph 3 to the Customer or the Competent Authorities, if so requested in writing.

3.6 The exit related obligations as provided in paragraph 11 (*Exit Assistance*) of *Regulatory Compliance* Schedule will apply in relation to the Services.

4. COOPERATION

4.1 The Providing Party will reasonably cooperate with the Ordering Party, the Customer or the Competent Authorities to allow the Customer to satisfy its DORA requirements, if requested by those entities and to the fullest extent required under DORA.

4.2 The abovementioned cooperation also includes the Providing Party's cooperation and participation in the Customer's testing of the Services, including in pooled ICT testing or threat-led penetration testing (TLPT). The Parties, and the Customer, if needed, will agree the terms of such Providing Party's participation in testing at least 30 days prior to the date of the tests, unless a shorter term is required under DORA.

5. DATA LOCATION

5.1 The Providing Party will provide the Ordering Party with information on any locations (countries or regions) from which the Providing Party or its Critical Subcontractors provide the Services or material part of them, and where the Customer's data are processed or stored in relation to the Services.

5.2 The Providing Party cannot change the country or the region from which the Services are provided, or where the Customer's data are processed or stored in relation to the Services, without notifying the Ordering Party at least 45 days in advance.

5.3 If the Customer affected by the above-mentioned change objects to it for reasonable and justified regulatory reasons, including cybersecurity concerns, the Ordering Party will inform the Providing Party of the objection. If the Providing Party upholds the proposed change and no other arrangement is agreed with the affected Customer within 30 days from the Customer's notification of its objection, the Customer will have the right to terminate its use of the Services affected by the change, and consequently the Ordering Party will have the right to terminate its use of the Services or their part that is provided to the Customer. The termination will be effective from the announced date of the Providing Party's implementation of the proposed change.

5.4 The Providing Party will not be entitled to any payment for the affected Services after the termination described above.

6. ADDITIONAL TERMINATION RIGHTS

6.1 The Ordering Party will have a right to terminate its use of the Services, or the part of them provided to the Customer, if the Customer terminates its use of the Ordering Party's services which include the Services due to a final and irrevocable decision of a Competent Authority ordering the Customer to terminate the Ordering Party's services for reasons attributable to the Providing Party, including a Competent Authority's decision that it can no longer effectively supervise the Customer as a result of the conditions of, or circumstances related to, the Services.

6.2 The termination referred to in this paragraph 6 will be effective as of the date the Ordering Party notifies the Providing Party of the effective termination by the Customer of the Ordering Party's services that include the Services.

6.3 The Providing Party will not be entitled to any payment for the terminated Services after the above-mentioned termination.

6.4 The termination rights referred to in this paragraph 6 are granted to the Ordering Party in addition to any other termination rights under the Agreement.

7. AUDIT, MONITORING AND NOTICE PERIODS

7.1 Upon the Customer's reasonable written request filed in order to comply with the Customer's regulatory obligations, the Providing Party will grant the Customer, its Auditor or a Competent Authority:

7.1.1 unrestricted rights of access, inspection and audit, and the right to take copies of relevant documentation on site if they are critical to the operations of the Providing Party related to the provision of the Services; and

7.1.2 the required cooperation during the onsite inspections and audits performed by the Auditor.

7.2 The Customer or its Auditor will execute a written confidentiality agreement acceptable to the Providing Party, or otherwise will be bound by a statutory or legal confidentiality obligation before executing their audit and access rights granted herein.

7.3 Lack of Compliance. If an audit reveals that the Providing Party is not compliant with the applicable laws or the Agreement, including this *Regulatory Compliance* Schedule, the Providing Party will at its own expense take any action needed to correct the identified non-compliance.

7.4 For the avoidance of doubt, the meaning and scope of the audit and access rights described above are to be interpreted in accordance with the provisions of DORA, the Regulatory Technical Standards issued under DORA and any applicable regulatory guidelines as amended or replaced from time to time.

8. INFORMATION OBLIGATIONS

8.1 At the Ordering Party's reasonable request, the Providing Party will provide to the Ordering Party, or indicate the source of, the following information:

8.1.1 up-to-date identification information (i.e. legal names, registered offices, corporate registration numbers, tax identification numbers, LEI numbers, etc.) on the Providing Party, its Critical Subcontractors and their ultimate parent companies;

8.1.2 other information or documentation that proves that the Providing Party and its Critical Subcontractors have the business reputation, sufficient abilities, expertise and adequate resources (financial, human and technical), as well as information security standards, appropriate organizational structure, risk management and internal controls, and authorizations or registrations (if applicable) needed to provide the Services in a reliable and professional manner;

8.1.3 information that is justifiably necessary to confirm that the Providing Party and its Critical Subcontractors comply with their obligations stipulated in this Annex;

8.1.4 reasonably requested information on the contractual documentation between the Providing Party and the Critical Subcontractors, and on relevant performance indicators.

8.2 If the Customer or a Competent Authority so requires under DORA, the Ordering Party can disclose to it information provided by the Providing Party under this paragraph 9, as well as information about the Providing Party and the Ordering Party's contractual arrangements with the Providing Party, including the contractual documentation.

9. CRITICAL SUBCONTRACTORS

9.1 The Providing Party must not subcontract its obligations under this Annex other than in accordance with paragraph 12 (*Assignment and Subcontracting*) of *Regulatory Compliance* Schedule. The following additional obligations apply with respect to Critical Subcontractors.

9.2 The Providing Party will:

9.2.1 flow down the obligations provided in this Annex to its Critical Subcontractors, including the obligation to grant the Auditors the same rights of access, inspection and audit as granted by the Customer under this Annex;

9.2.2 obligate its Critical Subcontractors to flow down the obligations provided in this Annex further to their Critical Subcontractors;

9.2.3 monitor the Critical Subcontractors' performance of subcontracted Services;

9.2.4 assess the risks associated with the locations of Critical Subcontractors and their parent companies, as well as the locations from which subcontracted Services are provided;

9.2.5 ensure the continuity of the Services in the event that a Critical Subcontractor fails to meet its obligations;

9.2.6 specify, in its agreement with each Critical Subcontractor, the ICT security standards and requirements that apply to the subcontracted Services.

9.3 Neither the Providing Party nor its Critical Subcontractors may change their subcontractors or material arrangements with them without obtaining Ordering Party's consent as required under paragraph 12 (*Assignment and Subcontracting*) of *Regulatory Compliance* Schedule.

9.4 If:

9.4.1 the Customer reasonably objects to any such proposed change in Critical Subcontractors or to material arrangements with them due to regulatory, including cybersecurity, concerns, and the Providing Party or its Critical Subcontractors nonetheless choose to implement the proposed change,

9.4.2 the Providing Party or its Critical Subcontractors subcontract Services whose subcontracting is not permitted under the Agreement,

and the Customer's use of the Services affected by the change is terminated, the Ordering Party will have the right to terminate its use of the Services or their part that is provided to the Customer, with effect from the effective date of implementation of the proposed change, of which the Ordering Party will immediately notify the Providing Party.

(End of Document)