VIRGIN MEDIA O2 SECURITY SCHEDULE

1. PURPOSE AND SCOPE

1.1 The purpose of this Security Schedule is to set out the minimum security standards to be met by third parties in their delivery of services, equipment, and software to VMO2 to ensure the integrity, security, resilience and confidentiality of VMO2 information and the VMO2 network.

1.2 This Security Schedule applies to all third parties who have access to any VMO2 information, its networks, systems, or environments (including involvement in design, implementation or development) and/or process or manage any VMO2 information.

1.3 The term "**VMO2**" in this Security Schedule refers to any member of the Virgin Media O2 Group who is the contracting entity and/or a recipient of the services, equipment, and software provided by the Supplier or its third parties pursuant to the Agreement.

1.4 The security requirements set out in this Security Schedule are in addition to and without prejudice to any other obligations of the Supplier in the Agreement.

2. DEFINITIONS

2.1 The following definitions shall apply to this Security Schedule:

Agreement	refers to the agreement which attaches this Security Schedule as an appendix or schedule or refers to this Security Schedule and is between the third party referred to at the start of the agreement (the "**Supplier**") and the VMO2 contracting entity.
Cloud Based Services	means any cloud hosting, cloud software, cloud support (including off-the-shelf, and pay as you go subscription cloud solutions) provided by the Supplier to VMO2.
Data Protection Legislation	means all applicable laws and regulations relating to the processing of personal data and privacy in the UK including the Data Protection Act 2018, the General Data Protection Regulation 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**GDPR**"), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any statutory instrument, order, rule or regulation made thereunder, as from time to time amended, extended, re-enacted or consolidated. The terms "personal data", "data controller", "data processor", "data subject" and "process" (in the context of usage of personal data) shall have the meanings given to them in the Data Protection Legislation.
Fourth Party Supplier	refers to any external entity or service provider that is engaged by a Third Party Supplier to perform services or functions that support the delivery of products or services to VMO2. Fourth Party Suppliers are indirectly involved in the supply chain and may have access to sensitive information or systems, necessitating the implementation of robust information security measures and risk management practices.
Good Industry Practice	means the exercise of the skill, care, prudence, efficiency, foresight and timeliness which would be expected from a highly skilled, trained and experienced person under the same or similar circumstances.
Services	means any equipment, software, services, media or documentation provided by the Supplier pursuant to the Agreement.
Supplier	has the meaning set out in the definition of Agreement above.
Third Party Supplier	means any subcontractor of the Supplier involved in the supply of the Services.
Virgin Media O2 Group	means VMED O2 UK Limited and any of its subsidiaries as defined in section 1159 of the Companies Act 2006.
VMO2 Information	means all and any personal data, customer data, employee data, confidential information, payment card data and/or other information or data provided to the Supplier and/or processed, stored or accessed by Supplier on behalf of VMO2 in connection with the Agreement. All references to the 'security' of VMO2 Information shall include the protection of the confidentiality, integrity, and continued availability of this information as applicable to the Services being provided.

2.2 All references to 'Supplier' shall include any employees, consultants, sub-contractors or agents or any other third parties carrying out any of the Services on behalf of the Supplier and Supplier shall be responsible for all such employees', consultants', sub-contractors' or agents' or any other third parties' compliance with this Security Schedule.

2.3 Any phrase with the expressions "including", "include", "in particular" or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

3. INFORMATION SECURITY

3.1 The Supplier's compliance with this Security Schedule and the implementation of any measures detailed in this Schedule is at the Supplier's cost unless otherwise stated in this Security Schedule.

3.2 The Supplier shall maintain an up-to-date document detailing what Services they provide to VMO2 and how these Services are used. This document must be made available to VMO2 within 30 days of written notice.

3.3 Without prejudice to any other notification obligations in this Security Schedule, the Supplier shall promptly advise VMO2 or their agents of any areas of non-compliance with VMO2 security requirements stated within this Security Schedule.

3.4 Further, the Supplier must inform VMO2 (via the Business Owner) prior to any changes to the Services to VMO2, that affect the ability of the Supplier to comply with this Security Schedule.

3.5 The Supplier shall implement and follow a formal change management process to ensure that changes to information processing facilities and systems are controlled.

3.6 The Supplier's information security will be compliant to ISO/IEC 27001. Evidence of compliance or certification to be provided to VMO2 upon written request as part of the information security questionnaire (paragraph 6.2) or the right to audit (section 13).

3.7 The Supplier shall design and implement processes that minimise the risk of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, VMO2 Information.

3.8 The Supplier must not implement any process or service which may put any VMO2 network, system or online services at risk.

3.9 Acceptance criteria for new information systems, upgrades, and new versions provided as part of the Services must be agreed with VMO2 and suitable tests of the system(s) carried out by the Supplier during development and prior to acceptance, in accordance with the Agreement.

3.10 Security configuration of services must be implemented in accordance with industry best practice security standards. The Centre for Internet Security (CIS) benchmarks (http://benchmarks.cisecurity.org) shall be used unless no relevant benchmark exists in which case manufacturer guidelines shall be used.

3.11 The Supplier shall arrange for independent annual security penetration testing of their services, by a CREST approved third party. All results that impact the Agreement shall be shared, upon reasonable request, with VMO2.

3.12 Web applications must be tested against the OWASP top ten risks (https://www.owasp.org).

3.13 A security patch management regime, with regular updates, must be implemented for the Services to ensure ongoing system integrity when new security vulnerabilities are discovered.

3.14 The Supplier shall maintain a list of any devices or media used by the Supplier to provide the Services to VMO2.

3.15 Where any devices and media are owned by VMO2, the Supplier shall adhere to VMO2 instructions to either return to VMO2 or destroy such devices or media if requested.

3.16 The Supplier shall secure its networks and access connections in accordance with Good Industry Practice to maintain appropriate protection of VMO2 Information.

3.17 The Supplier shall not use any 'live' VMO2 Information within a test, pre-production, or other non-live environment.

3.18 The Supplier shall ensure a "secure by default" approach to ensure standard builds and/or configurations for infrastructure and end user equipment (for example using build templates).

3.19 The Supplier shall ensure mail exchange is protected with TLS and set a DMARC policy, preferably DKIM signed. (DMARC – Domain-based Message Authentication, Reporting and Conformance is a technical standard that helps protect email senders and recipients from advanced threats that can be the source of an email data breach. DKIM – Domain Keys Identified Mail is an email authentication method designed to detect forged sender addresses in email, a technique often used in phishing and email spam).

3.20 The Supplier shall ensure secure transmission and storage of Information using strong cryptography and/or pseudonymization where appropriate, in accordance with Good Industry Practice.

3.21 The Supplier shall ensure appropriate measures are in place and maintained to secure the network infrastructure (e.g. Intrusion Detection Systems, use of 2-factor authentication for remote access, separation of networks, content filtering, encrypted network protocols, etc.).

4. DETECTION

4.1 The Supplier shall establish processes to keep up to date with emerging security threats and vulnerabilities and ensure that the relevant and appropriate security controls are implemented.

4.2 The Supplier shall implement appropriate measures to prevent and/or detect potential fraud in accordance with Good Industry Practice.

4.3 The Supplier shall ensure appropriate detection, prevention and recovery controls to protect against malicious code (e.g. without limitation, viruses) in all systems used to store or process VMO2 information or support the Services.

5. LEGAL & REGULATORY COMPLIANCE

5.1 Without prejudice to any other rights or remedies VMO2 may have, any material or persistent breach of this Security Schedule shall give rise to a right to VMO2 to immediately terminate the Agreement (or any part of it) for material breach. VMO2 may in its absolute discretion decide to allow the Supplier a remedial period of up to 30 days to remedy any such material or persistent breach, following which if the Supplier fails to remedy the breach, VMO2 may exercise its right to immediately terminate the Agreement (or any part of the Services).

5.2 For each information system, the Supplier shall explicitly define, document, and keep up to date all statutory and regulatory requirements relevant to the Services, and the Supplier's approach to meet these requirements.

5.3 All software used by the Supplier to discharge its obligations under the Agreement (with the exception of any software licensed to the Supplier by VMO2) must be validly owned or licensed by Supplier for the duration of the Agreement.

5.4 If applicable to the Services, Supplier shall comply with, and ensure that its agents and staff comply with, the provisions of the Official Secrets Acts 1911 to 1989 during the term of the Agreement and indefinitely after its expiry or termination.

5.5 It will be agreed as part of the Agreement where ownership of data lies, data processing activities, and the responsibilities of data controller and data processor. Data breaches shall be notified in accordance with paragraph 7.2 below.

5.6 The Supplier shall ensure that any service used to process and store VMO2 Information has the capability to extract and export such data quickly, normally within 5 working days (unless otherwise stated in the Agreement), in order to respond to a subject access request, which has been made in accordance with the Data Protection Legislation.

5.7 Additional legal and regulatory requirements are detailed in Appendix A to this Security Schedule as follows:

1.0 Payment Card Industry Security Standard (PCI DSS)

2.0 Sarbanes Oxley Compliance

3.0 Network and Information Systems Regulations 2018 (NIS)

4.0 Smart Metering

5.0 Resilience Controls

5.8 Additional legal and regulatory requirements relating to telecommunications security are detailed in Appendix B to this Security Schedule.

6. COMPLIANCE

6.1 The Supplier shall have a documented compliance plan and conduct regular reviews (at least annually) to ensure that the security of VMO2 Information cannot be compromised.

6.2 VMO2 may require the Supplier to complete an information security questionnaire as part of our Supplier review process, which may be subject to a full physical and logical information security review at all relevant Supplier locations in accordance with the Right to Audit section 13 below.

6.3 Except where otherwise stated in the Agreement or an applicable data processing agreement between the Supplier and VMO2, the Supplier must respond to any requests for information or data to be provided to VMO2 in relation to the Services and Supplier's compliance with this Security Schedule within 30 days of notice to the Supplier.

7. BREACHES AND COMPLIANCE FAILURES

7.1 The Supplier shall have sufficiently detailed and robust processes in place to ensure the prompt identification, investigation, and management of potential information security breaches and/or vulnerabilities of the Services. This shall include maintaining a documented security escalation process, which at a minimum shall set out a process to ensure compliance with the Supplier's notification obligation set out in paragraph 7.2.

7.2 The Supplier shall as soon as reasonably practicable (but by no later than 48 hours or as otherwise set out in the Agreement, or shorter if required by applicable law or regulation) inform VMO2 in writing of becoming aware of any VMO2 Information data breach. Data breach in this paragraph shall mean a breach of security or incident leading which has led to or could lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, VMO2 Information.

7.3 With the exception of data breaches, which shall be notified in accordance with paragraph 7.2 above, the Supplier shall promptly (but by no later than 5 business days) inform VMO2 in writing of becoming aware of any breach of the obligations set out in this Security Schedule.

7.4 Notifications required in this section 7 shall be notified by the Supplier to VMO2 by emailing security.incident@virginmediao2.co.uk

7.5 The Supplier shall provide, without delay, reasonable cooperation and assistance to VMO2 in the event of any data breach with respect to the VMO2 Information or non-compliance with the Supplier's obligations in this Security Schedule. In addition, the Supplier shall promptly

implement any measures required to correct such data breach or non-compliance with the Supplier's obligations in this Security Schedule.

7.6 Without prejudice to any other rights or remedies VMO2 may have in the Agreement or at law, VMO2 reserves the right to temporarily restrict or withdraw any Service where the Service is in breach of any of the obligations set out within this Security Schedule. In such an event the parties shall meet to agree remedial actions to remedy any such breaches. VMO2 shall not be liable to pay for any services(s) which are restricted or withdrawn pursuant to this paragraph.

7.7 VMO2 may contact the Supplier for technical support for assistance in resolving obligations associated with a data security breach or incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so.

8. RETENTION OF VMO2 INFORMATION

8.1 The Supplier shall treat all VMO2 Information provided to them as confidential, unless otherwise marked.

8.2 The Supplier shall comply with all obligations relating to confidential information set out in the Agreement.

8.3 The Supplier shall comply with VMO2 data retention policy (as amended from time to time). A copy of the policy is available at https://www.o2.co.uk/abouto2/supplier-contracting-policy-and-conditions

8.4 The Supplier shall logically segregate VMO2 Information and ensure the VMO2 Information can at all times be identified and distinguished, from the Supplier's or Supplier's other clients' data.

8.5 Except as otherwise stated in the Agreement and always in compliance with the Data Protection Legislation with respect to personal data, the parties agree, that at the request and choice of VMO2, the Supplier shall return all VMO2 Information and copies thereof to VMO2, or shall destroy all this Information within 30 days and certify to VMO2 that it has done so, unless legislation imposed upon the Supplier prevents the returning or destroying of all or part of the VMO2 Information transferred. In that case the Supplier warrants that it shall notify VMO2 of the Information being retained (including the reason for retention) and the Supplier shall maintain the confidentiality of the Information and shall not continue to actively process the VMO2 Information. This includes:

8.5.1 electronic, hard-copy and other media forms which contains information irrespective of the location;

8.5.2 any VMO2 Information retained by the Supplier's sub-contractors, or any third parties used by the Supplier in the provision of the Services.

8.6 Where there is a need to dispose of media that contains or stores VMO2 Information or other hard copies of data, the Supplier shall ensure it is disposed of securely and safely with the destruction certificates issued as required.

8.7 All items of equipment containing VMO2 Information on storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

9. ACCESS CONTROL

9.1 Access to networks and VMO2 Information must be adequately managed and controlled, in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit.

9.2 The Supplier shall ensure that all accesses to VMO2 Information are logged and linked to an accountable and identifiable person or machine process.

9.3 The Supplier shall put in place adequate controls to ensure that user actions and events cannot be deleted, removed, tampered with or modified in any way.

9.4 The Supplier shall ensure that processes exist to authorise, modify, and remove access to VMO2 Information. All such changes must be recorded.

9.5 The Supplier shall ensure that there is no sharing of account IDs and passwords or actual accounts.

9.6 The Supplier shall ensure that system access to VMO2 Information includes an automatic password protected inactivity time-out function that shall operate when the keyboard has not been used for in excess of 15 minutes at most.

9.7 The Supplier shall ensure all users follow Good Industry Practice in the selection, quality and use of passwords including the length, complexity and change frequency.

9.8 Full reviews of all accounts must be regularly undertaken, and access removed if not required on a regular basis.

9.9 The Supplier shall enforce separation of duties to avoid use of systems by users with conflicting roles, i.e. where a user can abuse its functions and also alter the audit trails. When separation of duties is not possible or practical, compensating controls must be put in place and recorded.

9.10 Access to data shall be available on a 'need to know' basis. It must not be possible for users (whether external or internal) to gain access to data that is not relevant to them.

9.11 A prescribed warning screen shall be displayed immediately after a user successfully completes the logon sequence. The system administrator shall set up procedures to provide written authorisation to users stating their access privileges.

9.12 Development, test and live operational facilities must be separated to reduce the risks of unauthorised access or changes to the live operational system.

9.13 Any system used to process data must not be connected to non-trusted networks without adequate security protection mechanisms (e.g. use of industry standard encryption).

9.14 Multi-factor authentication is required for remote access.

9.15 When logging into VMO2 systems Supplier shall ensure that its personnel are uniquely authenticated using only user identifications provided by VMO2, and that no system will be shared after user authentication.

9.16 The Supplier shall ensure that privileged user access management is implemented and maintained, ensuring that any privileged account activity on systems is carried out from dedicated separate accounts that are closely monitored and managed. Such privileged accounts must be reviewed regularly and always updated as part of the Suppliers joiners, movers, and leavers process.

10. BUSINESS CONTINUITY

10.1 The Supplier shall provide a copy of their business continuity policy and a business continuity plan that demonstrates how they will maintain the contracted levels of service in the event of an emergency. The Supplier's business continuity policy and planning with respect to the Services provided to VMO2 must align with the best practice detailed in the standard ISO 22301 Business Continuity Management.

10.2 The Supplier will send a copy of their business continuity policy and a business continuity plan to VMO2 using the email address businesscontinuity@virginmediao2.co.uk within 14 days of commencement of the Services.

10.3 The Supplier's business continuity policy and plan will be subject to an annual review by the Supplier and the updated documents will be forwarded to the same email address not more than 13 months following the previous submission.

10.4 VMO2, acting reasonably, reserves the right to request further information relating to Supplier's business continuity arrangements, including but not limited to exercise schedules and reports, and Suppliers will use all reasonable efforts to respond promptly to such information requests.

11. PHYSICAL SECURITY

11.1 The points of entry into the building used to process or store VMO2 Information shall be kept to an operational minimum. Where possible, all access shall be via the reception area.

11.2 Suitable access points shall be provided for goods delivery access.

11.3 Access to the areas used to process or store VMO2 Information shall be physically controlled (e.g. using an electronic access control system) including:

11.3.1 two factor authentication shall be used to manage access into computer rooms and other sensitive areas.

11.3.2 the system should log all activities, alarms and events and hold data for a minimum of 90 days.

11.3.3 the electronic access control system should be appropriately maintained.

11.4 Access to the areas processing or storing VMO2 Information should be restricted to authorised people working on the Agreement and particular Services or those who have an operational requirement to access the area.

11.5 Access rights to secure areas should be regularly reviewed and revalidated. Where access is no longer required, the rights should be revoked.

11.6 All final fire exit doors shall be physically secured. Other doors which form part of the external building shell shall be secure when not in use.

11.7 Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

11.8 There shall be a defined and documented procedure in place to manage visitors and temporary access into the building and internal areas used to process and manage VMO2 Information.

11.9 A suitable intruder detection system shall be installed to national or international standards and regularly maintained and tested.

11.10 An effective CCTV system shall be used to monitor the external building, the main reception area, any other staff entrance points, and the goods delivery point(s) and the system shall maintain a minimum of 30 days recording.

11.11 Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. These protections shall be appropriately maintained.

12. HUMAN RESOURCE SECURITY

12.1 The Supplier will perform thorough background verification checks on all employees and contractors who are involved in any way in the provision of the Services prior to them having access to any VMO2 Information, system or network related to the Services. Such checks shall be carried out in accordance with all applicable laws and regulations and Best Industry Practice, and shall include all checks required by the HMG BPPS (Baseline Personnel Security Standard) or equivalent including confirmation of the individual's identity, their right to work in the UK, 3 years of employment references and a criminal record check, together with any relevant qualifications, bankruptcy and/or CCJ checks, any appropriate health checks, and the passing of appropriate and valid security clearances.

12.2 The Supplier shall ensure that employees and contractors have no unspent criminal convictions which would question their honesty, integrity, and suitability to be employed for the purposes of the Agreement and/or the Services.

12.3 The Supplier shall comply with all reasonable requests made by VMO2 in respect of the deployment of individual employees engaged for the purposes of the Agreement and/or the Services including (i) participation in a candidate selection process, and (ii) the removal of individuals from the provision of the Services at VMO2's discretion.

12.4 The Supplier shall train, inform, and educate its employees and contractors about VMO2 information security requirements and best practice in relation to information security, and provide evidence thereof to VMO2 upon request.

12.5 The Supplier shall have written policies for employees when dealing with security measures and safe use of passwords.

12.6 The Supplier shall provide reasonable co-operation with VMO2 on fraud and security issues relating to any of their employees or contractors, having regard to all applicable regulation and legislation.

12.7 The Supplier shall ensure that each of its employees and contractors who are involved in the provision of the Services are bound by an appropriate confidentiality agreement covering the confidentiality obligations and information security of the Services and VMO2 Information.

12.8 The Supplier shall provide training to all employees and contractors on how to comply with the Supplier's physical, organisational, technical, and administrative information security safeguards and confidentiality obligations under this Agreement.

13. AUDIT

13.1 Without prejudice to any other right of audit that VMO2 may have, the Supplier shall permit VMO2, or an independent representative, to perform an audit by providing no less than 30 days' notice. The Supplier will allow VMO2 or its independent representative to enter any location used in connection with the Services being provided and provide VMO2 or its independent representative access to relevant personnel, data, policies, documentation and systems involved in the provision of the Services. The purpose of this audit is to inspect and verify the compliance of the Supplier with its obligations under this Security Schedule. VMO2 shall not conduct an audit more frequently than once in any 12 month period, except in the event VMO2 reasonably suspects a breach of the Supplier's obligations under this Security Schedule. For the avoidance of doubt, completion of the information security questionnaire shall not be considered an audit pursuant to this paragraph.

13.2 The Supplier shall carry out such tasks as are reasonably necessary to support VMO2's right to audit.

13.3 The Supplier shall permit VMO2 or an independent representative to undertake security penetration testing and / or vulnerability testing on any Service which is used to process VMO2's Information.

13.4 VMO2 reserves the right to carry out an exit audit where the Agreement has expired or terminated, including any partial termination, by providing the Supplier with a minimum of 30 days' notice. In the event of an exit audit the Supplier shall complete an exit audit questionnaire and submit its data processing facilities and that of its sub-processing facilities (e.g. third parties, sub-contractors, operating companies) for an audit by VMO2 or their appointed 3rd Party. The purpose of an exit audit is to inspect and verify the compliance of the Supplier with its obligations under this Security Schedule.

13.5 The Supplier shall, without delay, provide reasonable assistance and co-operation with VMO2 in implementing any measures required to remedy any non-compliance with Supplier's obligations set out in this Security Schedule, as detected in any audits carried out pursuant to this Section 13.

14. PORTABLE DEVICE SECURITY

14.1 Any portable device that is used to store or accesses VMO2 Information shall have the entire device encrypted to a minimum symmetrical standard of AES 256-bit encryption (e.g. laptops, tablets, smartphones, USB flash drives, memory sticks, and other removable media must have Advanced Encryption Standard (AES) as a minimum).

14.2 The device security shall ensure that:

14.2.1 temporary storage areas are encrypted;

14.2.2 decryption of the device is only allowed after successfully entering a passphrase/PIN unique to the device;

14.2.3 the entire device shall automatically encrypt after 15 minutes inactivity;

14.2.4 users are able to lock the device manually before periods of inactivity;

14.2.5 the passphrase used shall adhere to Good Industry Practice.

14.3 Where the entire device cannot be encrypted, all data contained within the device shall be encrypted to a standard approved by the VMO2 Security Team.

14.4 USB ports must be disabled for mass storage (memory sticks / memory cards) and require a business justification for their use. Where possible this use must be for a restricted amount of time, and then automatically removed.

14.5 In the event that portable devices are used, logging information will be stored to provide an audit trail of all storage devices that have been connected.

14.6 In the event of a lost or stolen storage device, the Supplier shall promptly, and in any event within 48 hours of becoming aware, notify VMO2 by emailing security.incident@virginmediao2.co.uk

14.7 In the event that portable devices are used, there should be an automatic process that erases data from the storage device after a maximum of 6 failed password attempts.

15. BACKUP

15.1 The Supplier shall ensure that VMO2 Information is protected against destruction, corruption or loss.

15.2 The Supplier must have appropriate backup and restore procedures in place that are in accordance with Good Industry Practice and fully documented and implemented to safeguard electronic VMO2 Information used or processed by the Supplier and ensure that VMO2

Information is recoverable within the relevant agreed recovery time and recovery point objectives in the event of destruction, loss and/or corruption. These procedures shall document the backup and recovery measures required for any supporting equipment and systems, and must include provision for the backup of elements such as:

15.2.1 Databases

15.2.2 Operating/ business systems

15.2.3 Configuration files and system-level information (including network elements such as routers, switches, firewalls etc.)

15.2.4 Firmware

15.2.5 Applications

15.2.6 Virtualised infrastructure

15.2.7 User-level data contained in the systems

15.2.8 Critical documentation including security related documentation

15.3 The Supplier shall implement measures to control availability of VMO2 Information by regularly reviewing and testing their backup and restore procedures as appropriate.

15.4 The Supplier shall ensure the design of systems, networks and application software provide facilities to take regular backups. The Supplier shall ensure these backup mechanisms are available and can be readily used to restore VMO2 Information and allow continued operation of VMO2 services.

15.5 The Supplier shall ensure the backup and restore procedures are part of business continuity and disaster recovery plans to ensure availability of VMO2 Information following interruption to, or failure of, any VMO2 services.

15.6 The Supplier shall ensure the scope and frequency of backups are commensurate with the nature and criticality of the VMO2 Information being stored.

15.7 The Supplier shall ensure copies of VMO2 Information are routinely reviewed, to ensure backup media reliability, integrity and availability of the information needing to be recovered.

15.8 The Supplier shall ensure the backup copy of VMO2 Information, and a copy of the Supplier backup and restore procedures referred to in Section 1.2 are kept in a place different from the location of the systems that process the information, which MUST always comply with the security measures of the original location and using protective measures that guarantee information integrity and recovery to ensure that recovery is possible.

16. VULNERABILITY MANAGEMENT

16.1 Vulnerability identification – The Supplier shall ensure that they are aware of any security weakness, both through proactive registration to the Supplier or industry alert services and through reactive logging of findings from technical audits.

16.2 Vulnerability response – The Supplier shall ensure that their response to the notification of a vulnerability and identification of a mitigation is commensurate to the threat vector and reported severity of the vulnerability. Supplier shall triage vulnerabilities to determine if appropriate mitigations are already implemented or if delivery of mitigations are required within said

response time. The Common Vulnerability Scoring System (CVSS) version 3.x will be used to define response times as follows:

- Critical vulnerabilities (CVSS 9.0-10)
    - 14 days from notification of vulnerability (for external interfaces)
    - 30 days from notification of vulnerability (for internal interfaces)
- High vulnerabilities (CVSS 7.0-8.9)
    - 30 days from notification of vulnerability (for external interfaces)
    - 90 days from notification of vulnerability (for internal interfaces)
- Other vulnerabilities (CVSS below 6.9)
    - 90 days from notification of vulnerability (for external interfaces)
    - As part of normal patching cycle (for internal interfaces)

16.3 The Supplier shall analyse potential effects on existing systems and services from implementation of vulnerability mitigations, coordinating this activity with other groups including, but not confined to:

- Release management
- Change management
- Service management
- Product management

16.4 Vulnerability mitigation – mitigations to vulnerabilities can either take the form of a patch, configuration or other control and shall be treated as requests that will include a required period of time for their implementation. The Supplier must maintain documentary evidence on response and mitigation details (including details of patches, configurations or other controls and their implementation details) and supply such evidence on VMO2's request.

16.5 The Supplier shall participate in meetings and committees relating to the security process as reasonably requested by VMO2 to coordinate delivery of vulnerability mitigations.

16.6 The Supplier shall ensure any software developed by the Supplier is developed using OWASP secure coding guidelines.

16.7 The Supplier shall ensure any software developed by the Supplier is tested every six months for security flaws and to create workarounds or patches to mitigate the vulnerability according to the requirements in 16.2.

16.8 The Supplier shall not change the software version or level of patching on any part of the solution without prior agreement from VMO2.

16.9 The Supplier shall maintain an up to date list detailing all software applications that are required as part of the Services for support purposes. The Supplier shall provide the list to VMO2 upon written request.

16.10 The Supplier shall have a documented roadmap of future software implementation showing versions and “end of life” or “end of support” detail in order to avoid the solution retaining out of date software for any longer than necessary. This includes any third party software included in the Services.

16.11 The Supplier shall treat any “end of life” or “end of support” notification as a critical vulnerability and react accordingly.

16.12 Except as otherwise set out in the Agreement, the Supplier shall document any third party software required for the Services and shall, upon request, supply VMO2 with evidence to show that support is available for this third party software for the lifetime of the Service.

16.13 The Supplier shall ensure that software/applications shall not be part of a version lock, therefore preventing regular updates and patches.

16.14 Where the Supplier provides custom code to VMO2, the code will be static application security tested (SAST) and dynamic application security tested (DAST).

16.15 The Supplier shall perform continuous vulnerability scanning on any of the Supplier’s assets (internal or external) that create, store, transport, process, or delete VMO2 Information.

17. LOGGING & MONITORING

17.1 The Supplier shall ensure that all access to VMO2 Information is recorded in an electronic audit log, which can only be viewed by authorised people.

17.2 The Supplier shall protect logging facilities and log information from tampering and unauthorised access.

17.3 The Supplier shall protect and regularly review system administrator and system operator activities of systems that have access to VMO2 Information.

17.4 The Supplier shall facilitate the complete and secure maintenance and retention of activity log record’s. Logs shall be retained for a minimum of 12 months.

17.5 The Supplier shall support VMO2 with the analysis and understanding of log information.

17.6 The Supplier shall ensure that clocks of all information processing systems are synchronised to a single reference time source.

17.7 The Supplier shall ensure that Root (or shared accounts including those with Administrator access) cannot be used without traceability to an individual user.

18. FOURTH PARTY SUPPLIERS

18.1 The Supplier shall conduct a comprehensive risk assessment prior to onboarding any new Fourth Party Supplier. This assessment shall evaluate the potential risks associated with the Fourth Party Supplier’s information security practices and overall risk profile.

18.2 The Supplier shall perform ongoing risk assessments of all Fourth Party Suppliers. These assessments shall be conducted at regular intervals and shall include a review of the Fourth Party Supplier’s information security practices, compliance with relevant standards, and any changes in their risk profile.

18.3 The Supplier shall ensure that an agreement is entered into between the Supplier and the Fourth Party Supplier and that all such agreements with Fourth Party Suppliers include specific information security requirements. These requirements shall , as a minimum, address the

protection of sensitive data, compliance with applicable laws and regulations, and adherence to industry best practices for information security.

18.4 The Supplier shall have a documented process in place to regularly monitor, review, evaluate, and manage changes in the information security practices of Fourth Party Suppliers. This process shall include mechanisms for identifying, notifying and addressing any potential security vulnerabilities or compliance issues that may arise.

19. CLOUD SECURITY

19.1 When the Supplier is providing Cloud Based Service, these clauses will apply.

19.2 The Supplier must document and implement clearly defined processes for acquisition, use, management and exit from Cloud Based Services.

19.3 The Supplier will ensure that the Cloud Based Services support Transport Layer Security (TLS) version 1.2 or above and ensure that they are configured to use cipher suites and certificate sizes recommended by the NCSC - https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data

19.4 The Supplier will ensure that no versions of the Secure Sockets Layer (SSL) protocol are used.

19.5 The Supplier must encrypt all VMO2 Information stored in the Cloud Based Service when in transit and at rest using industry-standard encryption algorithms (e.g., AES-256).

19.6 The Supplier will ensure that all internet-facing ways of accessing the Cloud Based Service will require successful authentication using Good Industry Practice authentication methods.

19.7 The Supplier will ensure that Cloud Based Services that are accessed over the internet, and which process VMO2 Information, implement a method of 2-factor authentication (2FA) or multi factor authentication (MFA) to the Service.

19.8 The Supplier will implement the following access measures:

19.8.1 appropriate levels of account privilege and have authorisation mechanisms in place to enforce the separation of privileges between different types of account.

19.8.2 role-based access control to ensure that users only have access to the resources necessary for their role and that these are regularly reviewed.

19.9 The Supplier will ensure that the Cloud Based Service generates all relevant security logs. Security logs should include, without limitation: authentication attempts, configuration changes, and details about resources being accessed. All security logs will be made available to VMO2 promptly upon request. Such security logs shall be retained by the Supplier for a minimum of 13 months and must be protected against tampering and unauthorised access.

19.10 The Supplier will ensure that the Cloud Based Services are monitored for unauthorised access or unauthorised activity.

19.11 The Supplier will have a clearly defined policy for applying security updates to its internal systems and responding to identified security issues in accordance with Good Industry Practice.

19.12 The Supplier will apply security updates and patches to the Cloud Based Services in a timely manner, following a risk-based approach to prioritize critical vulnerabilities in accordance with Good Industry Practice.

19.13 The Supplier will ensure that VMO2 Information will only be stored in the UK, or within the EEA, unless approved in writing by the VMO2 Security Team.

19.14 The Supplier will ensure that any Cloud Based Services used to process VMO2 Information has an annual penetration test, by a CREST approved third party. All results that impact the Cloud Based Services and the Supplier's obligations under the Agreement shall promptly be shared with VMO2.

19.15 The Supplier must have a clearly documented incident response plan for security incidents affecting the Cloud Based Services.

19.16 The Supplier will implement and maintain a Cloud Security Posture Management (CSPM) solution to continuously monitor and manage the security posture of the cloud environment. The CSPM solution should detect and alert on misconfigurations, vulnerabilities, and compliance issues, and provide actionable remediation steps.

APPENDIX A TO THE VIRGIN MEDIA O2 SECURITY SCHEDULE

ADDITIONAL LEGAL, REGULATORY AND CONTRACTUAL REQUIREMENTS

1. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

1.1 Where the Supplier is transmitting, storing and or processing Payment Card Data, the Supplier shall comply with this Appendix A, Section 1.0.

1.2 The Supplier must ensure that they comply with all card scheme rules and regulations, including but not limited to the most recent version of the Payment Card Industry Data Security Standard ("**PCI DSS**") as promulgated by the Payment Card Standards Security Council ("**PCI SSC**") as updated from time to time and as they apply to the Services. VMO2 require proof of such compliance by an externally signed Attestation of Compliance (AoC) at which time the Supplier shall provide that proof within 1 month. The Supplier shall perform regular reviews of their security, availability and processing integrity, reporting to VMO2 any identified vulnerability per PCI DSS requirements.

1.3 The Supplier agrees and acknowledges that they are responsible for the security of cardholder data and the Supplier shall indemnify VMO2 from and against all penalties, costs and expenses which may be suffered, paid, or incurred by VMO2 as a consequence of the Supplier's failure to comply with the PCI DSS requirements.

1.4 The Supplier shall limit storage amount and retention time of card holder data to that which is required for business, legal, and/or regulatory purposes, as required by VMO2's data retention policy.

1.5 The Supplier shall perform an annual PCI compliance assessment for all work relating to VMO2 and provide an externally signed Attestation of Compliance within 1 month.

1.6 In the event of an Attestation of Compliance failure, the Supplier must perform any remedial action required within a timescale agreed with VMO2.

2. SARBANES OXLEY COMPLIANCE

2.1 Pursuant to rules adopted by the United States' Securities and Exchange Commission ("**SEC**") implementing section 404 of SOX it is understood by the parties that the SEC requires VMO2 to include in its annual report (and/or the annual reports of other companies in the VMO2 Group on form 20-F ("**Annual Report**") a report of management on internal controls over financial reporting.

2.2 It is further understood by the parties that the VMO2's auditor (and/or the auditors of other companies in the Telefónica UK Group) shall be required to issue an attestation report on management's assessment of internal control over financial reporting and the attestation report shall be filed as part of the Annual Report (the "**Filing**").

2.3 Where relevant to the Services, the Supplier may be required to provide information applicable to VMO2's compliance requirements in paragraphs 2.1 and 2.2 above.

3. NETWORK AND INFORMATION SYSTEMS REGULATIONS (NIS) 2018

3.1 The Supplier shall, where requested by VMO2, work with VMO2 to achieve compliance to government requirements for digital service providers (as defined in the NIS regulations).

3.2 The Supplier agrees to provide reasonable assistance and cooperation to VMO2 to ensure compliance with the NIS Regulations.

4. SMART METERING

4.1 The Supplier shall be independently certified to ISO27001:2013, with a scope that covers Smart Metering Data.

5. RESILIENCE CONTROLS

If Appendix B (Telecommunications Security) of this Security Schedule applies to the Supplier, then the requirements of this Section 5 do not apply.

5.1 For each Agreement with VMO2, the Supplier must carry out an appropriate resilience risk assessment and disclose it to VMO2.

5.2 The Supplier must recognise and minimise the risks of security breaches in the VMO2 's network or services caused by the Supplier's services or facilities.

5.3 The Supplier agrees to let VMO2 observe all of their actions related to the VMO2 network or services.

5.4 The Supplier shall provide a point of contact for incident management for support and escalation of incidents.

5.5 The Supplier shall immediately (but no later than 48 hours) report and escalate all security incidents, vulnerabilities and misuse that could cause security risks to VMO2 in accordance with the VMO2 corporate information security policy and all technical or administrative security rules or procedures that arise from it.

5.6 The Supplier shall report on the root cause of any security incident within 30 days, and rectify any weaknesses found. Where the Supplier cannot quickly resolve weaknesses, the Supplier shall work with VMO2 to ensure the issue is mitigated until resolved.

5.7 The Supplier will ensure all VMO2 Information is handled by appropriate employees and transferred or exchanged via secure and authenticated channels which are appropriately encrypted according to industry standards.

5.8 The Supplier shall be required to verify that VMO2 Information is properly protected, through the right to audit.

5.9 The Supplier shall ensure that any administrator controls they apply are at least as rigorous as VMO2 controls when the administrator has access to VMO2's network or service or to sensitive VMO2 Information.

5.10 The Supplier shall ensure that network and service security is preserved throughout the termination and changeover of the contract with VMO2.

5.11 The Supplier must state whether fuzz testing is performed and provide a description of the scale of this testing.

APPENDIX B TO THE VMO2 SECURITY SCHEDULE

TELECOMMUNICATIONS SECURITY

PART 1: TSA SUPPLIERS (EXCLUDING OUTSOURCED INFRASTRUCTURE SUPPLIERS)

CONTENTS

1. PURPOSE AND SCOPE

1.1 This Appendix B, Part 1 forms part of the Virgin Media O2 Security Schedule and identifies additional obligations that apply to Suppliers who supply, provide or make available goods, services or facilities pursuant to the Agreement for use in connection with the provision of any VMO2 Public Electronic Communications Network or VMO2 Public Electronic Communications Services ("**TSA Suppliers**"). This Appendix shall not apply to Outsourced Infrastructure Suppliers to the extent the Outsourced Infrastructure Suppliers are providing Services in respect of Outsourced Infrastructure such that the obligations in Appendix B, Part 2 would apply.

1.2 Any Supplier to which this Appendix applies must be able to demonstrate adherence to the requirements contained in this Appendix which are intended to reflect the latest guidance from the Telecommunications Security Code of Practice published by the UK Government Department for Digital, Culture, Media & Sport Telecommunications in December 2022 (the "**Code of Practice**") which in turn sets out and details the security measures contained within the Regulation and the TSA (both as defined in Paragraph 2 below). Both VMO2 and the Supplier agree that the requirements within this Appendix may be updated by VMO2 from time to time to reflect changes to the Code of Practice, the Regulation and/or the TSA.

1.3 In the event of a conflict between the requirements in this Appendix, the Security Schedule or any other security requirements that VMO2 may have specified, then the most stringent requirement shall be applied.

1.4 The Supplier shall:

1.4.1 be responsible for all acts and omissions of its Third Parties as fully as if they were the acts and omissions of the Supplier or its employees or agents;

1.4.2 ensure that all applicable requirements in this Appendix are contractually imposed on Third Parties in written contractual agreements so as to (i) enable the Supplier to comply with its obligations under this Appendix and (ii) ensure that Third Parties are subject to the same security requirements as the Supplier. For the avoidance of doubt, this includes where the Supplier is required to provide support, information and/or assistance to VMO2 pursuant to the requirements in this Appendix, in which case the Supplier shall contractually impose all necessary requirements on its Third Parties to provide the Supplier with all and any support, information and/or assistance required to enable the Supplier to fulfil its obligations to VMO2.

1.5 All obligations with respect to Network and User Data are without prejudice to any other Supplier obligations in the Agreement and any other agreement between VMO2 and the Supplier relating to data processing.

2. DEFINITIONS

2.1 Except as otherwise defined within this Paragraph 2 or this Security Schedule of which this Appendix forms part, this Appendix shall incorporate the definitions set out in the Code of Practice, the Regulation and the TSA.

2.2 For the avoidance of doubt, references to "this Appendix" in this Appendix B, Part 1 shall refer to this Appendix B, Part 1.

2.3 The following definitions shall apply to this Appendix:

Agreement	has the meaning set out in the definitions section of this Security Schedule.
Business Day	means a day (other than a Saturday or Sunday) except for public holidays in England.
Code of Practice	has the meaning set out in Paragraph 1.2 of this Appendix.
Customer Premises Equipment or CPE	refers to equipment provided to VMO2's customers, that is used, or intended to be used, as part of the VMO2 network or service. This excludes consumer electronic devices such as mobile phones and tablets, but does include devices such as edge firewalls, SD-WAN equipment, and fixed wireless access kit.
Listed Country or Listed Countries	means countries listed in the schedule to the Regulation for the purposes of regulations 5(3) and 8(6), as amended or replaced from time to time.
Managed Service Provider	means any entity that delivers services, such as network, application, infrastructure and security, via ongoing and regular management, support and active administration on VMO2's premises, in Supplier's data centre (hosting), or in a third party data centre.
Network and User Data	means VMO2 network data, and VMO2 Information including, for the avoidance of any doubt, VMO2's end-user data.
Network Equipment	means either a software or hardware component of VMO2's network that transmits or receives data or provides supporting services to components of the VMO2's network that transmit or receive data. It includes both virtual machines and physical hardware.
OEM	means original equipment manufacturer.

PECN or Public Electronic Communications Network	has the meaning set out in sections 32 and 151 of the Communications Act 2003 as amended from time to time.
PECS or Public Electronic Communications Service	has the meaning set out in sections 32 and 151 of the Communications Act 2003 as amended from time to time.
Regulation	means the Electronic Communications (Security Measures) Regulations 2022 as amended from time to time.
Regulator	means any person or body having regulatory, supervisory or governmental authority over telecommunications services including but not limited to the Office of Communications or any of their successors from time to time.
Security Compromise	means, in relation to any VMO2 PECN or VMO2 PECS, the events set out in The Communications Act 2003 Section 105A Subsection (2)(a) to (2)(g) subject to the exclusions set out in The Communications Act 2003 Section 105(A) Subsection (3) as updated from time to time.
Services	has the meaning set out in the definitions section of this Security Schedule.
Third Party Administrators (3PA)	means Managed Service Providers, provider of group functions, or external support for Network Equipment (e.g. third-line support function).
Third Party or Third Parties	means any subcontractor, contractor, agent or third party, not a party to the Agreement, which is involved directly or indirectly in the supply chain of the Services provided by the Supplier to VMO2. Third Parties shall also include any OEMs involved in the provision of products and services to VMO2.
TSA	means the Telecommunications (Security) Act 2021 as amended from time to time.
VMED O2 UK Group Member	means VMED O2 UK Limited or each legal entity registered in the United Kingdom, that is a Subsidiary (as defined in section 1159 of the Companies Act 2006) of VMED O2 UK Limited from time to time.
VMO2 Information	has the meaning set out in the definitions section of this Security Schedule.
VMO2 PECN or VMO2 Public Electronic Communications Network	means any PECN provided by the VMO2 contracting entity to the Agreement or any VMED O2 UK Group Member.
VMO2 PECS or VMO2 Public Electronic Communications Service	means any PECS provided by the VMO2 contracting entity to the Agreement or any VMED O2 UK Group Member.

3. GENERAL PROVISIONS RELATING TO INFORMATION, ASSISTANCE AND AUDIT

3.1 Information and Assistance

3.1.1 The Supplier shall provide all reasonable assistance, information and cooperation to enable VMO2 or any VMED O2 UK Group Member to respond to (i) any notice, direction and/or information request issued to VMO2 or any VMED O2 UK Group Member by any Regulator, and/or (ii) any audit or assessment carried out by, or on behalf of, any Regulator in respect of VMO2 or any VMED O2 UK Group Member. Such assistance and cooperation shall be provided in accordance with any reasonable timeframe required by VMO2 to enable VMO2 to comply with any timeframes stipulated by any Regulator.

3.1.2 The Supplier shall provide, upon written request from VMO2, copies of or access to any logs, records or information kept by the Supplier as required by this Appendix, within twenty (20) Business Days (unless otherwise agreed by the Supplier and VMO2) of such request.

3.1.3 Where the Supplier is required to provide any information, data, updates or documents pursuant to this Appendix and unless stated otherwise in the relevant Paragraph in this Appendix, such information, data, updates or documents shall be provided to the relevant Agreement business contact at VMO2 via an encrypted and authenticated channel.

3.2 Audit

3.2.1 For the purposes of this Appendix, Section 13 (Audit) of the Security Schedule shall not apply.

3.2.2 Without prejudice to any other audit rights of VMO2 detailed in the Agreement, VMO2 may (itself or via its statutory auditors, authorised agents, accountants, qualified personnel, consultants and/or any Regulators from time to time) audit the Supplier's compliance with this Appendix (including audits of the Supplier premises, data centres, systems, data, policies and records relating to the provision of the Services). Such audits shall be limited to once every twelve (12) months other than where VMO2 has reasonable grounds to believe that the Supplier is not complying with its obligations under this Appendix or where an audit is required by applicable law or requested by a Regulator.

3.2.3 In connection with any such audit, the Supplier shall (i) provide to the auditing party such unimpeded access (including to Supplier personnel) and co-operation as reasonably requested for the purposes of the audit and (ii) procure all reasonable assistance and access to Third Party personnel for the purposes of the audit.

3.2.4 Where VMO2 has reasonable grounds to believe that the Supplier is not complying with its obligations under this Appendix or where an audit is required by applicable law or requested by a Regulator, an audit may be carried out without prior notice. Where reasonably practicable, VMO2 will provide advance notice of such an audit. In all other circumstances VMO2 shall provide at least twenty (20) Business Days' notice to the Supplier prior to any audit being conducted.

3.2.5 VMO2 may engage third party advisers who are not competitors of the Supplier, to undertake any audit.

3.2.6 In exercising its rights under this Paragraph 3.2, VMO2 shall use reasonable endeavours to:

(a) ensure that any audit, inspection or verification is conducted during the hours of normal operation of the Supplier's business (or as otherwise agreed by the parties from time to time);

(b) as far as is commercially practicable, minimise disruption to the Supplier's business; and

(c) procure that any auditing party which is a third party of VMO2 (other than its personnel or a Regulator) enters into a non-disclosure undertaking.

3.2.7 In the event an audit identifies non-compliances with the requirements of this Appendix, without prejudice to any other rights or remedies of VMO2 or any VMED O2 UK Group Member, VMO2 may require the remediation of such non-compliances in accordance with the provisions of the Agreement.

4. MEASURES APPLICABLE TO ALL TSA SUPPLIERS

4.1 The Supplier shall have clear, exercised and implemented processes for managing security incidents, at varying levels of severity.

4.2 The Supplier shall use lessons learned from previous security incidents to inform the security of new products and services offered to VMO2.

4.3 Where providing installation and/or configuration services, the Supplier shall remove or change default passwords and accounts for all devices in the network and disable unencrypted management protocols. Where unencrypted management protocols cannot be disabled, Suppliers shall limit and mitigate the use of these protocols as far as possible.

4.4 Where providing installation and/or configuration services, the Supplier shall ensure that all security-relevant logging is enabled on all Network Equipment used in the provision of a VMO2 PECN or VMO2 PECS and sent to the network logging systems.

4.5 The Supplier shall provide assistance to VMO2 (as reasonably requested by VMO2) in the creation of a clear and documented shared-responsibility model between the Supplier and VMO2.

4.6 The Supplier's incident management process and that of their Third Parties shall provide mutual support in the resolution of incidents.

4.7 The Supplier shall define what VMO2 Information is made accessible to any of its Third Parties, ensuring that it is the minimum necessary to fulfil their function. The Supplier shall place controls on that VMO2 Information and limit Third Party access to the minimum required to fulfil the business function.

4.8 When making Network and User Data available to Third Parties outside of a secure Privileged Access system, the Supplier's environment that is used to hold and make the Network and User Data available to the Third Party shall be secure and segregated from the Supplier's wider systems and data.

4.9 The Supplier shall avoid transferring control of any Network and User Data to Third Parties, except where necessary. Any such transfer of control should be limited to the necessary and defined purpose. Where a transfer of any Network and User Data is necessary, it shall be through a defined process.

4.10 Where Network and User Data leaves a Supplier's control, the Supplier shall contractually require and verify that the Network and User Data is properly protected as a consequence. This shall include assessing the Third Parties' controls to ensure the Network and User Data is only visible or accessible to appropriate employees and from appropriate locations.

4.11 When sharing Network and User Data, the Supplier and its Third Parties shall use an encrypted and authenticated channel.

4.12 The Supplier shall promptly (but by no later than 48 hours) notify VMO2 of becoming aware of any security incidents that may have caused or contributed to the occurrence of a Security Compromise or where an increased risk of such a Security Compromise occurring has been identified. This includes, but is not limited to, incidents in the Supplier's development network or its corporate network. Such notification shall include details of the relevant security incident and the Supplier incident reference number. The Supplier shall promptly provide information relating to the security incident or increased risk as reasonably requested by VMO2.

4.13 The Supplier shall provide VMO2 with all reasonable support and assistance in investigations of incidents that cause or contribute to the occurrence of a security compromise in relation to VMO2, or of an increased risk of such a compromise occurring.

4.14 The Supplier shall find and report to VMO2 in writing via email to security.incident@virginmediao2.co.uk on the root cause within 30 days of any security incident that could result in a Security Compromise and rectify any security failings found.

4.15 Where the Supplier cannot quickly resolve security failings, the Supplier shall work with VMO2 and provide all reasonable support and assistance to VMO2 to ensure that any incidents or security failings or issues are mitigated until resolved. The Supplier shall keep VMO2 regularly informed (via email to security.incident@virginmediao2.co.uk) of progress towards resolution of any security failings, including details of any mitigations and confirmation of resolution.

4.16 If the Supplier does not resolve any security failings within a reasonable timeframe, VMO2 shall be entitled to terminate the Agreement without penalty and without any liability for early termination.

4.17 Without prejudice to Paragraph 3.2 of this Appendix, the Supplier shall support, as far as appropriate, any security audits, assessments or testing required by VMO2 in relation to the security of any VMO2 PECN and/or VMO2 PECS, including without limitation those necessary to evaluate the security requirements of this TSA Appendix.

Listed Countries

4.18 The Supplier must ensure that any tools (a) are not capable of being accessed from a Listed Country, and (b) are not stored on equipment located in a Listed Country. Tools shall cover tools that enable (a) the monitoring or analysis in real time of the use or operation of the network or service, or (b) the monitoring or analysis of the content of signals (Regulation 5(3)).

4.19 The Supplier must ensure that (a) no Security Permission is given to a person while the person is in a Listed Country, and (b) any Security Permission cannot be exercised while the person to whom it is given is in a Listed Country (Regulation 8(6)).

4.20 The Supplier shall ensure that contingency procedures are in place in the event that further locations are added to the schedule of Listed Countries in the Regulation.

5. MEASURES APPLICABLE TO TSA SUPPLIERS THAT ARE THIRD PARTY ADMINISTRATORS

5.1 The Supplier shall prioritise critical security patches over functionality upgrades wherever possible.

5.2 VMO2 shall retain the rights to determine the permissions of the accounts used by either the Supplier or its Third Parties to access the VMO2 network.

5.3 The Supplier acknowledges that VMO2 retains the right to control the access granted to Supplier personnel who are involved in the provision of the Services including the ability to remove access.

5.4 The Supplier acknowledges that the Supplier and/or its Third Parties shall not have routine, direct access to Network Equipment. Any access shall be via mediation points owned and operated by VMO2.

5.5 The Supplier shall implement technical controls to prevent VMO2 or its network from adversely affecting any other provider or their network, and to prevent any other provider or their network from adversely affecting VMO2 or its network. Such technical controls shall include:

5.5.1 logical separation within the Third Party Administrator network to segregate customer data and networks;

5.5.2 separation between Third Party Administrator management environments used for different provider networks;

5.5.3 limitation of the potential for users or systems to negatively impact more than one provider;

5.5.4 logically-independent Privileged Access Workstations per provider;

5.5.5 independent administrative domains and accounts per provider.

5.6 The Supplier shall ensure that, security enforcing functions are implemented and enforced at the boundary between the Supplier network and the VMO2 network.

5.7 The Supplier shall monitor and audit the activities of its staff when accessing VMO2's network.

5.8 The Supplier shall maintain for a minimum of 12 months, and provide VMO2 with ongoing access to, all logs relating to the security of its network to the extent that such logs relate to access into VMO2's network.

5.9 The Supplier shall ensure that its networks that could impact VMO2 undergo independent annual security penetration testing of their services by a CREST approved third party and any other reasonable testing requirements as required by VMO2. All results that impact the Services shall be shared, upon reasonable request, with VMO2.

5.10 The Supplier shall ensure that any patches or updates carried out by the Supplier do not affect the patched equipment's ability to meet all relevant obligations set out in this TSA Appendix throughout its lifecycle, including after an upgrade or patch.

5.11 The Supplier shall ensure that operational, network or system changes are only implemented according to VMO2 formal change processes.

5.12 The Supplier shall use appropriately skilled and dedicated resources to understand and analyse security-related network activity.

5.13 The Supplier shall protect the integrity of logging data and any modification shall be alerted and attributed.

5.14 The Supplier shall ensure all actions involving stored logging or monitoring data (e.g. copying, deleting, modification or viewing) are traceable back to an individual user.

5.15 Where the Supplier provides installation and/or configuration services in respect of Customer Premise Equipment, the Supplier shall ensure that:

5.15.1 each item of CPE is configured to contain credentials that are both unique to that CPE, and not guessable from CPE metadata.

5.15.2 Wide Area Network CPE management interfaces shall only be accessible from specified management locations (e.g. URL or IP address).

5.15.3 management of the CPE uses a secure protocol that has not been deprecated (e.g. TLS 1.2 or newer).

5.15.4 by default, the CPE's customer-facing management interfaces shall only be accessible from within the customer's network.

5.15.5 by default, all unsolicited incoming connections towards the customer's network shall be blocked by the CPE.

6. MEASURES APPLICABLE TO TSA VENDORS THAT PROVIDE NETWORK EQUIPMENT

6.1 The Supplier shall provide to VMO2 details of all major components used in the provision of the Services, and promptly (and in any event within twenty (20) Business Days) respond to any requests for further information from VMO2 in relation to such details.

6.2 The Supplier must provide to VMO2 a "security declaration", signed off by an authorised representative of the Supplier, that explains how the Supplier produces secure equipment and maintains the equipment's security throughout its lifetime. The declaration should also record any differences in process across product line. It is a requirement that any such declaration cover all aspects described within Annex B of the Code of Practice.

6.3 Where the Supplier has obtained any recognised security assessments or certifications of their Network Equipment they shall share with VMO2 the full findings that evidence this assessment or certificate.

6.4 The Supplier must maintain and adhere to, as a minimum, the standards set out in its 'security declaration' and supply up-to-date guidance to VMO2 on how Network Equipment should be securely deployed.

6.5 The Supplier will support all Network Equipment and all software and hardware subcomponents used in the provision of goods and services to VMO2 for the term of the Agreement.

6.6 Prior to the commencement of the Agreement and in any event within thirty (30) days of the commencement date of the Agreement, the Supplier shall provide details (product and version) of, and maintain such details of, major third-party components and dependencies, including open-source components and the period and level of support. Any changes to such details shall be notified to VMO2 in writing.

6.7 The Supplier shall remediate any security issues that pose a security risk to the VMO2 network or service discovered within the Supplier's product(s), or any third party supplier's product(s), within a reasonable timeframe, providing regular updates until resolution. This shall include all products impacted by the security issue, not only the product for which the security issue was reported.

6.8 The Supplier shall promptly notify VMO2 of any failures by Supplier or its Third Parties to meet the obligation in Paragraph 6.7.

6.9 The Supplier authorises VMO2 to share details of security issues to be shared as appropriate to support the identification and reduction of the risks of security compromises occurring in relation to the VMO2 PECN or VMO2 PECS as a result of things done or omitted by the Supplier or its Third Parties.

6.10 The Supplier shall deliver critical security patches separately to feature releases, to maximise the speed at which the patch can be deployed.

6.11 The Supplier shall ensure that Network Equipment is delivered in a secure-by-default configuration based on the principle that only required services are made available.

6.12 The Supplier shall ensure that any patches or updates carried out by the Supplier do not affect the patched equipment's ability to meet all relevant obligations set out in this Appendix throughout its lifecycle, including after an upgrade or patch.

6.13 The Supplier shall have in place a vulnerability disclosure policy that includes, at a minimum, a public point of contact and details around timescales for communication.

7. MEASURES APPLICABLE TO TSA SUPPLIERS THAT ARE PROVIDING SIM CARDS

7.1 The Supplier shall ensure that only SIM credentials and SIM transport keys are stored within secured systems that ensure data integrity and prevent 'read' access to key material.

7.2 The Supplier shall ensure that when transferring the VMO2's SIM key material from SIM Card vendors, a range of transport keys shall be used, and not shared, across multiple SIM Card vendor customers.

7.3 When the Supplier defines new SIM Card authentication algorithm parameters (e.g. for MILENAGE (a set of authentication and key generation functions proposed by the 3rd Generation Partnership Project)), the default values shall not be used.

7.4 For Fixed-profile SIMs, the Supplier shall ensure that sensitive SIM data is appropriately protected throughout its lifecycle by the SIM Card vendor, given the risk to network resilience and confidentiality should this information be lost.

7.5 For Fixed-profile SIMs, the Supplier shall ensure that the confidentiality, integrity and availability of the sensitive SIM Card data shared with the SIM Card vendor shall be protected at every stage of their lifecycle.

7.6 For Fixed-profile SIMs, the Supplier shall ensure that the security of the SIM Card vendor has been independently audited. For example, using the GSMA's SAS scheme provides a means to accredit the security of SAS suppliers.

7.7 The Supplier shall ensure that all new UICCs can be updated with new K/Ki and OTA keys after receipt from the SIM Card vendor.

8. MEASURES APPLICABLE TO TSA VENDORS THAT PROVIDE CUSTOMER PREMISE EQUIPMENT

8.1 The Supplier shall ensure that each item of CPE delivered by the Supplier contains credentials that are both unique to that CPE, and not guessable from CPE metadata.

8.2 The Supplier shall inform VMO2 of any plans to cease support of CPE in accordance with any timeframe set out in the Agreement.

ANNEX TO APPENDIX B, PART 1

CODE OF PRACTICE AND APPENDIX REFERENCING

Code of Practice measure number	Corresponding Appendix Paragraph	Code of Practice measure number	Corresponding Appendix Paragraph	Code of Practice measure number	Corresponding Appendix Paragraph
M5.04	4.1	M10.25	5.5.1	M10.38	6.2
M5.07	4.2	M10.26	5.5.2	M10.39	6.3
M8.06	4.3	M10.28	5.5.3	M10.40	6.4
M8.07	4.4	M10.29	5.5.4	M10.41	6.4
M10.03	4.5	M10.30	5.5.5	M10.42	6.5
M10.04	4.6	M10.27	5.6	M10.43	6.6
M10.06	4.7	M10.33	5.7	M10.44	6.7
M10.07	4.8	M10.34	5.8	M10.45	6.8
M10.08	4.9	M10.35	5.9	M10.46	6.9
M10.09	4.10	M10.53	5.10	M10.47	6.10
M10.10	4.11	M11.01	5.11	M10.48	6.11
M10.11	4.12	M16.01	5.12	M10.53	6.12
M10.12	4.13	M16.08	5.13	M10.54	6.13
M10.13	4.14	M16.09	5.14	M4.06	7.1
M10.14	4.15	M9.01	5.15.1	M8.10	7.2
M10.15	4.16	M9.03	5.15.2	M8.11	7.3
M10.16	4.17	M9.04	5.15.3	M8.12	7.4
M8.08	5.1	M9.05	5.15.4	M8.13	7.5
M10.18	5.2	M9.06	5.15.5	M8.14	7.6
M10.21	5.3	M10.01	6.1	M8.15	7.7
M10.22	5.4	M10.36	6.2	M9.01	8.1
M10.24	5.5	M10.37	6.2	M9.02	8.2

APPENDIX B TO THE VIRGIN MEDIA O2 SECURITY SCHEDULE

TELECOMMUNICATIONS SECURITY

PART 2: OUTSOURCED INFRASTRUCTURE SUPPLIERS

CONTENTS

1. PURPOSE

1.1 This Appendix B, Part 2 forms part of the Virgin Media O2 Security Schedule and identifies additional obligations that apply to Suppliers which take responsibility for part of the infrastructure that is used to support any VMO2 Public Electronic Communications Network and/or VMO2 Public Electronic Communication Services (including Supplier equipment and services supplied in connection with that infrastructure and including any such infrastructure provided by the Supplier's Third Parties (as defined in Paragraph 2 below)) ("**Outsourced Infrastructure**") and provided by the Supplier pursuant to the Agreement ("**Outsourced Infrastructure Suppliers**"). Outsourced Infrastructure Suppliers are required to adhere to all of the regulations, management and oversight requirements that would apply to VMO2 in relation to Outsourced Infrastructure to the extent that the Outsourced Infrastructure Suppliers are responsible for that Outsourced Infrastructure.

1.2 Any Supplier to which this Appendix applies must be able to demonstrate adherence to the requirements contained in this Appendix which are intended to reflect the latest guidance from the Telecommunications Security Code of Practice published by the UK Government Department for Digital, Culture, Media & Sport Telecommunications in December 2022 (the "**Code of Practice**") which in turn sets out and details the security measures contained within the Regulation and the TSA (both as defined in Paragraph 2 below). Both VMO2 and the Supplier agree that the requirements within this Appendix may be updated by VMO2 from time to time to reflect changes to the Code of Practice, the Regulation and/or the TSA.

1.3 In the event of a conflict between the requirements in this Appendix, the other obligations set out in this Security Schedule or any other security requirements that VMO2 may have specified, then the most stringent requirement shall be applied.

1.4 The Supplier shall:

1.4.1 be responsible for all acts and omissions of its Third Parties as fully as if they were the acts and omissions of the Supplier or its employees or agents;

1.4.2 ensure that all applicable requirements in this Appendix are contractually imposed on Third Parties in written contractual agreements so as to (i) enable the Supplier to comply with its obligations under this Appendix and (ii) ensure that Third Parties are subject to the same security requirements as the Supplier. For the avoidance of doubt, this includes where the Supplier is required to provide support, information and/or assistance to VMO2 pursuant to the requirements in this Appendix, in which case the Supplier shall contractually impose all necessary requirements on its Third Parties to provide the Supplier with all and any support, information and/or assistance required to enable the Supplier to fulfil its obligations to VMO2.

1.5 All obligations with respect to Network and User Data are without prejudice to any other Supplier obligations in the Agreement and any other agreement between VMO2 and the Supplier relating to data processing.

2. DEFINITIONS

2.1 Except as otherwise defined within this Paragraph 2 or this Security Schedule of which this Appendix forms part, this Appendix shall incorporate the definitions set out in the Code of Practice, the Regulation and the TSA. For the purposes of this Appendix, any references to 'provider' in the definitions in the Code of Practice, the Regulation and the TSA shall refer to the Supplier. This shall not affect any reference to 'provider' within the body of this Appendix, including the definitions in this Appendix.

2.2 For the avoidance of doubt, references to "this Appendix" in this Appendix B, Part 2 shall refer to this Appendix B, Part 2.

2.3 The following definitions shall apply to this Appendix:

Agreement	has the meaning set out in the definitions section of this Security Schedule.
Business Day	means a day (other than a Saturday or Sunday) except for public holidays in England.
Code of Practice	has the meaning set out in Paragraph 1.2 of this Appendix.
Corporate Security Domain	a system or group of systems that all have the same level of security which protects the Supplier's own data and any VMO2 data processed by the Supplier.
Incoming Signal	means any signal received by the Supplier network.
Listed Country or Listed Countries	means countries listed in the schedule to the Regulation for the purposes of regulations 5(3) and 8(6), as amended or replaced from time to time.
Network and User Data	means Supplier network data, VMO2 Information including, for the avoidance of any doubt, VMO2's end-user data.
Network Equipment	either a software or hardware component of the Supplier's network that transmits or receives data or provides supporting services to components of the Supplier's network that transmit or receive data. It includes both virtual machines and physical hardware.
Network Oversight Functions	means the components of the network that oversee and control the Security Critical Functions and systems that collect and process logging and monitoring data. Network Oversight Functions include, but are not limited to, the following components of the network where such components oversee and control Security Critical Functions: element managers; virtualisation orchestrators; management systems (e.g. Jump Boxes); security functions (e.g. firewalls at the edge of a security zone); root authentication services (e.g. active directories (ADs)); Multi-

	Factor Authentication services; security gateways (e.g. supporting the Management Plane); audit and monitoring systems (including network quality monitoring of speech and data); and Operational Support Systems (OSSs).
OEM	means original equipment manufacturer.
Outsourced Infrastructure	has the meaning set out in Paragraph 1.1 of this Appendix.
Outsourced Infrastructure Supplier	has the meaning set out in Paragraph 1.1 of this Appendix.
PECN or Public Electronic Communications Network	has the meaning set out in sections 32 and 151 of the Communications Act 2003 as amended from time to time.
PECS or Public Electronic Communications Service	has the meaning set out in sections 32 and 151 of the Communications Act 2003 as amended from time to time.
Regulation	means the Electronic Communications (Security Measures) Regulations 2022 as amended from time to time.
Regulator	means any person or body having regulatory, supervisory or governmental authority over telecommunications services including but not limited to the Office of Communications or any of their successors from time to time.
Security Compromise	means, in relation to the Supplier's networks and the Supplier's services respectively, to the extent that they affect any VMO2 PECN or VMO2 PECS, the events set out in The Communications Act 2003 Section 105A Subsection (2)(a) to (2)(g) subject to the exclusions set out in The Communications Act 2003 Section 105(A) Subsection (3) as updated from time to time.
Security Critical Function	means any function of the Supplier's network or services whose operation is likely to have a material impact on the proper operation of the Supplier's entire network or service or a material part of it.
Sensitive Data	means (a) data which controls, or significantly contributes to, a Security Critical Function, or (b) data which is the content of a signal.
Services	has the meaning set out in the definitions section of this Security Schedule.
Third party Administrators (3PA)	means Managed Service Providers, Supplier group functions, or external support for Third Party Supplier Equipment (e.g. third-line support function).
Third Party or Third Parties	means any subcontractor, contractor, agent or third party, not a party to the Agreement, which is involved directly or indirectly in the supply chain of the Services provided by the Supplier to VMO2. Third Parties shall also include any OEMs involved in the provision of products and services to VMO2.
TSA	means the Telecommunications (Security) Act 2021 as amended from time to time.

VMED O2 UK Group Member	means VMED O2 UK Limited or each legal entity registered in the United Kingdom, that is a Subsidiary (as defined in section 1159 of the Companies Act 2006) of VMED O2 UK Limited from time to time.
VMO2 Information	has the meaning set out in the definitions section of this Security Schedule.
VMO2 PECN or VMO2 Public Electronic Communications Network	means any PECN provided by the VMO2 contracting entity to the Agreement or any VMED O2 UK Group Member.
VMO2 PECS or VMO2 Public Electronic Communications Service	means any PECS provided by the VMO2 contracting entity to the Agreement or any VMED O2 UK Group Member.

3. GENERAL PROVISIONS RELATING TO INFORMATION, ASSISTANCE AND AUDIT

3.1 Information and Assistance

3.1.1 The Supplier shall provide all reasonable assistance, information and cooperation to enable VMO2 or any VMED O2 UK Group Member to respond to (i) any notice, direction and/or information request issued to VMO2 or any VMED O2 UK Group Member by any Regulator, and/or (ii) any audit or assessment carried out by, or on behalf of, any Regulator in respect of VMO2 or any VMED O2 UK Group Member. Such assistance and cooperation shall be provided in accordance with any reasonable timeframe required by VMO2 to enable VMO2 to comply with any timeframes stipulated by any Regulator.

3.1.2 The Supplier shall provide, upon written request from VMO2, copies of or access to any logs, records or information kept by the Supplier as required by this Appendix, within twenty (20) Business Days (unless otherwise agreed by the Supplier and VMO2) of such request.

3.1.3 Where the Supplier is required to provide any information, data, updates or documents pursuant to this Appendix and unless stated otherwise in the relevant Paragraph in this Appendix, such information, data, updates or documents shall be provided to the relevant Agreement business contact at VMO2 via an encrypted and authenticated channel.

3.2 Audit

3.2.1 For the purposes of this Appendix, Section 13 (Audit) of the Security Schedule shall not apply.

3.2.2 Without prejudice to any other audit rights of VMO2 detailed in the Agreement, VMO2 may (itself or via its statutory auditors, authorised agents, accountants, qualified personnel, consultants and/or any Regulators from time to time) audit the Supplier's compliance with this Appendix (including audits of the Supplier premises, data centres, systems, data, policies and records relating to the provision of the Outsourced Infrastructure). Such audits shall be limited to once every twelve (12) months other than where VMO2 has reasonable grounds to believe that the Supplier is not complying with its obligations under this Appendix or where an audit is required by applicable law or requested by a Regulator.

3.2.3 In connection with any such audit, the Supplier shall (i) provide to the auditing party such unimpeded access (including to Supplier personnel) and co-operation as

reasonably requested for the purposes of the audit and (ii) procure all reasonable assistance and access to Third Party personnel for the purposes of the audit.

3.2.4 Where VMO2 has reasonable grounds to believe that the Supplier is not complying with its obligations under this Appendix or where an audit is required by applicable law or requested by a Regulator, an audit may be carried out without prior notice. Where reasonably practicable, VMO2 will provide advance notice of such an audit. In all other circumstances VMO2 shall provide at least twenty (20) Business Days' notice to the Supplier prior to any audit being conducted.

3.2.5 VMO2 may engage third party advisers who are not competitors of the Supplier, to undertake any audit.

3.2.6 In exercising its rights under this Paragraph 3.2, VMO2 shall use reasonable endeavours to:

(a) ensure that any audit, inspection or verification is conducted during the hours of normal operation of the Supplier's business (or as otherwise agreed by the parties from time to time);

(b) as far as is commercially practicable, minimise disruption to the Supplier's business; and

(c) procure that any auditing party which is a third party of VMO2 (other than its personnel or a Regulator) enters into a non-disclosure undertaking.

3.2.7 In the event an audit identifies non-compliances with the requirements of this Appendix, without prejudice to any other rights or remedies of VMO2 or any VMED O2 UK Group Member, VMO2 may require the remediation of such non-compliances in accordance with the provisions of the Agreement.

4. MEASURES APPLICABLE TO ALL OUTSOURCED INFRASTRUCTURE SUPPLIERS

Overarching Security Measures

4.1 The Supplier shall maintain accurate records of all Externally-Facing Systems.

4.2 The Supplier shall arrange for security testing to be carried out on all Externally Facing Systems, excluding Customer Premises Equipment, at least every two years and in any case shortly after a significant change occurs.

4.3 The Supplier shall ensure that any equipment in the Exposed Edge shall not host Sensitive Data or Security Critical Functions.

4.4 The Supplier shall ensure that physical and logical separation is implemented between the Exposed Edge and Security Critical Functions.

4.5 The Supplier shall ensure that security boundaries are in place between the Exposed Edge and critical or sensitive functions that implement protective measures.

4.6 The Supplier shall ensure that equipment in the Exposed Edge shall not be able to impact operation or routing within the core network.

Management Plane Measures 1

4.7 The Supplier shall ensure that Privileged Access rights are regularly reviewed and updated as part of business-as-usual management. This shall include updating Privileged User rights in

line with any relevant changes to roles and responsibilities within the Supplier organisation or any access by Third Parties.

4.8 The Supplier shall ensure that all Privileged Access is logged. The Supplier shall ensure that all Privileged Access shall be via secure, encrypted and authenticated protocols whenever technically viable.

4.9 The Supplier shall ensure that management protocols that are not required are disabled on all network functions and equipment.

4.10 The Supplier shall ensure that default passwords are changed upon initialisation of any devices or services and before their use for the provision of the relevant network or service.

4.11 The Supplier's responsibility for the Outsourced Infrastructure shall include retaining oversight of the management of that Outsourced Infrastructure including sight of management activities, personnel granted Management Access, and management processes.

Third Party Supplier Measures 1

4.12 The Supplier shall ensure that, when engaging Third Parties to procure services and/or equipment for use in VMO2's PECN or VMO2's PECS, all risks included in Regulation 7(3) are assessed and that this assessment is documented and provided to VMO2 prior to contract or when requested by VMO2. In doing so, the Supplier should, as a minimum, refer to the guidance contained in NCSC's Vendor Security Assessment to assess Third Parties (as contained in Annex B of the Code of Practice). This assessment shall inform both risk management and procurement processes.

4.13 The Supplier shall record all equipment that remains in use but has reached the Vendor's End-Of-Life Date. The Supplier shall regularly review their use of this equipment, with a view to reducing the risk of a Security Compromise occurring as a result of unsupported equipment remaining in use.

4.14 The Supplier shall produce a plan to replace unsupported equipment at an appropriate time, dependent on the level of risk.

4.15 The Supplier shall record all risk management processes undertaken. Guidance on risk management processes can be found on the NCSC website.

Supporting Business Processes Measures

4.16 The Supplier shall implement appropriate business processes. In order to achieve this, the Supplier shall have regard to implementing the parts of the Cyber Assessment Framework that define the Supplier's business processes. These are contained within Annex C of the Code of Practice. These are: A1-Governance; A2-Risk Management; A3-Asset Management; B5-Resilient Networks and Systems; B6-Staff Awareness and Training; D1-Response and Recovery Planning; D2-Lessons Learned.

4.17 The Supplier shall prioritise security changes and minimise postponements of security changes. Where security changes are postponed, these shall be recorded as a business risk by the Supplier as appropriate.

4.18 The Supplier shall maintain read-only backups of their infrastructure and information and shall be able to restore them. The backups should contain the information necessary to maintain the normal operation of the public electronic communications network or public electronic communications service.

4.19 The Supplier shall have clear, exercised and implemented processes for managing security incidents, at varying levels of severity.

4.20 The Supplier shall perform a root-cause analysis of all security incidents. Outcomes of this analysis shall be escalated to an appropriate level within the Supplier's organisation and to VMO2 in accordance with the Agreement.

4.21 The Supplier shall use lessons learned from previous security incidents to inform the security of new products and services offered to VMO2.

Management Plane Measures 2

4.22 The Supplier shall store non-persistent credentials (e.g. username and password authentication) in a centralised service with appropriate role-based access control which shall be updated in line with any relevant changes to roles and responsibilities within the organisation.

4.23 The Supplier shall ensure that Privileged Access is via accounts with unique user ID and authentication credentials for each user and shall ensure that these unique user ID and authentication credentials are not shared.

4.24 The Supplier shall ensure that, for accounts capable of making changes to Security Critical Functions, the following measures are adopted relating to multi-factor authentication: (a) the second factor is locally generated, and not transmitted; and (b) the Multi-Factor Authentication mechanism is independent of the Supplier's network and PAW. Soft tokens (e.g. authenticator apps) may be used.

4.25 The Supplier shall ensure that all break-glass Privileged User accounts have unique, strong credentials per individual piece of Network Equipment.

4.26 The Supplier shall ensure that default and hardcoded accounts are disabled.

Third Party Supplier Measures 2

4.27 The Supplier shall perform appropriate and proportionate security testing in accordance with the TSA and the Regulation on any equipment used in the provision of Services to VMO2 and in all cases ensure that such security testing is passed prior to deployment of such equipment.

4.28 The Supplier shall supply written evidence to VMO2 on request of any tests carried out under Paragraph 4.27. Any third party testing in relation to the security of the Network Equipment shall only be accepted as evidence if it is repeatable, performed independently of the Network Equipment supplier and is clearly applicable to the Supplier’s deployment (e.g. relates to the hardware, software and configuration that is being supplied).

4.29 The Supplier shall record all equipment deployed in its networks, and proactively assess, at least once a year, their exposure should Third Parties be unable to continue to support that equipment.

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

4.31 The Supplier shall ensure that all security-relevant logging is enabled on all Network Equipment used in the provision of the Services and sent to the network logging systems.

4.32 The Supplier shall prioritise critical security patches over functionality upgrades wherever possible.

Third Party Supplier Measures 3

4.33 The Supplier shall maintain records of its Third Parties' details and the major components which are used in the provision of goods, services and/or facilities for VMO2.

4.34 The Supplier shall clearly express the security needs placed on its Third Parties. These shall be defined and agreed in contracts.

4.35 The Supplier shall ensure there is a clear and documented shared-responsibility model between the Supplier and their Third Parties.

4.36 The Supplier's incident management process and that of their Third Parties shall provide mutual support in the resolution of incidents.

4.37 The Supplier shall retain control and oversight of Services being provided to VMO2 including their Network and User Data that is used and/or processed in the delivery of those Services.

4.38 The Supplier shall define what information is made accessible to any Third Parties, ensuring that it is the minimum necessary to fulfil their function. The Supplier shall place controls on that information and limit Third Party access to the minimum required to fulfil the business function.

4.39 When making Network and User Data available to Third Parties outside of a secure Privileged Access system, the Supplier's environment that is used to hold and make the Network and User Data available to the Third Parties shall be secure and segregated from the Supplier's wider systems and data.

4.40 The Supplier shall avoid transferring control of the Network and User Data to Third Parties, except where necessary. Any such transfer of control should be limited to the necessary and defined purpose. Where a transfer of any Network and User Data is necessary, it shall be through a defined process.

4.41 Where any Network and User Data leaves the Supplier's control, the Supplier shall contractually require and verify that the Network and User Data is properly protected as a consequence. This shall include assessing the Third Parties' controls to ensure the Network and User Data is only visible or accessible to appropriate employees and from appropriate locations.

4.42 When sharing Network and User Data, the Supplier shall use an encrypted and authenticated channel.

4.43 The Supplier shall promptly (but by no later than 48 hours) notify VMO2 in writing via email to security.incident@virginmediao2.co.uk of becoming aware of any security incidents that may have caused or contributed to the occurrence of a Security Compromise, or where an increased risk of such a Security Compromise occurring has been identified. This includes, but is not limited to, incidents in the Supplier's development network or its corporate network. Such notification shall include details of the relevant security incident and the Supplier incident reference number. The Supplier shall promptly provide information relating to the security incident or increased risk as reasonably requested by VMO2.

4.44 The Supplier shall provide VMO2 with all reasonable support and assistance in investigations of incidents that cause or contribute to the occurrence of a Security Compromise, or of an increased risk of such a Security Compromise occurring.

4.45 The Supplier shall find and report to VMO2 in writing via email to security.incident@virginmediao2.co.uk on the root cause within 30 days of any security incident that could result in a Security Compromise and rectify any security failings found.

4.46 Where the Supplier cannot quickly resolve security failings, the Supplier shall ensure that any incidents or security failings or issues are mitigated until resolved. The Supplier shall keep VMO2 regularly informed (via email to security.incident@virginmediao2.co.uk) of progress towards resolution of any security failings, including details of any mitigations and confirmation of resolution.

4.47 If the Supplier does not resolve any security failings within a reasonable timeframe, VMO2 shall be entitled to terminate the Agreement or the relevant Service(s) without penalty and without any liability for early termination.

4.48 Without prejudice to Paragraph 3.2 of this Appendix, the Supplier shall support as far as appropriate, any security audits, assessments or testing required by VMO2 in relation to the security of any VMO2 PECN and/or VMO2 PECS, including without limitation those necessary to evaluate the security requirements of this Appendix.

4.49 The Supplier shall adopt appropriate security measures and apply controls that are at least as rigorous as the requirements in the sections of the Security Schedule when its personnel or its Third Party Administrators have access to the Supplier's network or to Sensitive Data.

4.50 The Supplier shall retain the right to determine permissions of the accounts used to access its network by Third Party Administrators and allow VMO2 to determine the permissions of the accounts (if any) used by either the Supplier or by its Third Parties to access the VMO2 network.

4.51 The Supplier shall ensure that they retain sufficient in-house expertise and technical ability to re-tender their managed services arrangements at any time and shall produce and maintain a plan for moving the provided services back in-house or to another Third Party.

4.52 The Supplier shall maintain an up-to-date list of all Third Party Administrator personnel that are able to access its network, including their roles, responsibilities and expected frequency of access.

4.53 Where reasonably requested by VMO2, the Supplier shall make changes to the access granted to members of Supplier personnel and/or personnel of its Third Parties who are involved in the provision of the Services to VMO2. Such changes may include without limitation the addition or removal of access to members of personnel.

4.54 The Supplier shall not allow routine, direct access to its Network Equipment by Third Party Administrators. Access shall be via mediation points owned and operated by the Supplier.

4.55 The Supplier shall implement and enforce security enforcing functions at the boundary between the Third Party Administrator network and the Supplier network.

4.56 The Supplier shall implement technical controls to prevent VMO2 from adversely affecting any other provider or their network, and to prevent any other provider or their network from adversely affecting VMO2. Such technical controls shall include:

4.56.1 logical separation within the Third Party Administrator network to segregate customer data and networks;

4.56.2 separation between Third Party Administrator management environments used for different provider networks;

4.56.3 limitation of the potential for users or systems to negatively impact more than one provider;

4.56.4 logically-independent Privileged Access Workstations per provider;

4.56.5 independent administrative domains and accounts per provider.

4.57 The Supplier shall ensure that the elements of Supplier network that are accessible by any Third Party Administrators shall be the minimum required to perform their contractual function.

4.58 The Supplier shall log and record all Third Party Administrator access to its networks and retain those logs for a suitable period.

4.59 The Supplier shall ensure that its Third Party Administrators monitor and audit the activities of their staff when accessing the Supplier's network.

4.60 The Supplier shall require from any of its Third Party Administrators all logs relating to the security of the Third Party Administrator's network to the extent that such logs relate to access into the Supplier's network and/or the Services provided to VMO2.

4.61 The Supplier shall require that networks of any of its Third Party Administrators that could impact the Supplier undergo the same level of testing as the Supplier applies to themselves, using a CREST approved third party.

4.62 The Supplier shall require its Third Parties supplying Network Equipment to share with them a 'security declaration' (signed off by an authorised representative) on how they produce secure equipment and ensure they maintain the equipment's security throughout its lifetime. The declaration should also record any differences in process across product line. Any such declaration should cover all aspects described within the NCSC's Vendor Security Assessment (VSA) in Annex B of the Code of Practice.

4.63 The Supplier shall ensure that where any of its Third Parties supplying Network Equipment involved in the provision of the Services claims to have obtained any internationally recognised security assessments or certifications of their equipment (such as the industry standards: 'Common Criteria' or 'NESAS'), the Supplier shall require such equipment suppliers to share with them the full findings that evidence this assessment or certificate. The Supplier shall provide any such evidence on request by VMO2.

4.64 The Supplier shall ensure that any of its Third Parties supplying Network Equipment (i) adhere to a standard no lower than the Third Party's security declaration shared pursuant to Paragraph 4.62; and (ii) supply up-to-date guidance on how the equipment should be securely deployed.

4.65 The Supplier shall ensure that any of its Third Parties supplying Network Equipment support all equipment and all software and hardware subcomponents for the length of the Agreement with VMO2. The period of support of both hardware and software shall be written into the contract.

4.66 The Supplier shall ensure that any of its Third Parties supplying Network Equipment provide and maintain details (product and version) of major third-party components and dependencies, including open-source components and the period and level of support.

4.67 Where relevant to the Supplier's particular usage of equipment, the Supplier shall contractually require its Third Parties to remediate all security issues that pose a security risk to the Supplier's network or service discovered within their products within a reasonable time of being notified, 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.

4.68 The Supplier shall record where its Third Parties fail to meet the security obligations set out in Paragraph 4.67.

4.69 The Supplier shall ensure that its contracts allow details of security issues to be shared as appropriate to support the identification and reduction of the risks of security compromises occurring in relation to its network or service as a result of things done or omitted by its Third Parties.

4.70 The Supplier shall contractually require its Third Parties supplying Network Equipment to deliver critical security patches separately to feature releases, to maximise the speed at which the patch can be deployed.

4.71 The Supplier shall ensure that their equipment is delivered in a secure-by-default configuration based on the principle that only required services are made available.

4.72 The Supplier shall ensure that all deployed equipment in its network either meets the Third Parties recommended secure configuration (as a minimum), or that any variations are recorded and the risk assessed.

4.73 The Supplier shall implement necessary mitigations based on identified equipment risks (e.g. use of an out-of-support component), such that these equipment risks do not increase the overall risk to their networks.

4.74 The Supplier shall update all supported equipment within such period as is appropriate of any relevant and appropriate version being released.

4.75 The Supplier shall 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. In addition, the Common Vulnerability Scoring System (CVSS) shall be used to define response times as follows:

Exposed, actively exploited vulnerabilities in the wild:

As soon as can reasonably be achieved and no longer than 14 days from notification (for external interfaces and internal interfaces)

Critical vulnerabilities (CVSS 9.0-10)

14 days from notification of vulnerability (for external interfaces)

30 days from notification of vulnerability (for internal interfaces)

High vulnerabilities (CVSS 7.0-8.9)

30 days from notification of vulnerability (for external interfaces)

90 days from notification of vulnerability (for internal interfaces)

Other vulnerabilities (CVSS below 6.9)

90 days from notification of vulnerability (for external interfaces)

As part of normal patching cycle (for internal interfaces)

To the extent that the Supplier is unable to deploy patches in line with the above timeframes, 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 Supplier shall ensure that such patches are deployed as soon as can reasonably be achieved, and at most within 14 days of release.

4.76 The Supplier shall ensure that any patches or updates do not affect the patched equipment's ability to meet all relevant obligations set out in this Appendix throughout its lifecycle, including after an upgrade or patch.

4.77 The Supplier shall verify that their Network Equipment suppliers have a vulnerability disclosure policy. This shall include, at a minimum, a public point of contact and details around timescales for communication.

Management Plane Measures 3

4.78 The Supplier shall ensure that all operational changes are only made according to a formal change process except under emergency or outage situations.

4.79 The Supplier shall ensure that any persistent credentials and secrets (e.g. for break glass access) are protected and not available to anyone except for the responsible person(s) in an emergency.

4.80 The Supplier shall ensure that central storage for persistent credentials shall be protected by hardware means. For example, on a physical host the drive could be encrypted with the use of a Trusted Platform Module. Where a virtual machine (VM) is used to provide a central storage service, the VM and the data included in it shall also be encrypted, use secure boot and be configured to ensure that it can only be booted within an appropriate environment. This is to ensure that data cannot be removed from the operational environment and accessed.

4.81 The Supplier shall ensure that:

4.81.1 Privileged Users are only granted specific privileged accounts and associated permissions which are essential to their business role and function;

4.81.2 Privileged Access is temporary, time-bound and associated with a specific trouble ticket;

4.81.3 while open, tickets are updated daily as a record of why Privileged Access granted to a user remains required and shall be closed once Privileged Access is no longer required.

4.81.4 all Privileged Access shall be revoked prior to ticket closure.

4.81.5 administrators shall not be able to grant themselves Privileged Access to the network.

4.82 The Supplier shall ensure that Privileged User accounts are generated from a least privilege role template and modified as required. The permissions associated with this account shall not be copied from existing users.

4.83 The Supplier shall ensure that a risk assessment is conducted for administrators performing multiple roles and having multiple accounts for this purpose.

4.84 When an emergency occurs, security requirements may temporarily be suspended. The Supplier shall perform clean-up steps after the emergency is resolved to ensure that the suspension of these requirements has not compromised the network. Where an ‘emergency’ event occurs, this shall be recorded and audited, along with the reason and time period for which controls were suspended.

4.85 The Supplier shall manage all "break glass" security accounts, ensuring that they are only used for emergency purposes outside of change windows. The Supplier shall raise an alert when they are used, investigate the circumstances and audit all activity logs. Such credentials shall be replaced after a single use.

4.86 The Supplier shall ensure that all Privileged Access activity undertaken during a management session shall be fully recorded.

4.87 The Supplier shall ensure that a device that is not necessary to perform network management or support management operations shall not be able to logically access the Management Plane.

4.88 The Supplier shall ensure that Privileged Access to Network Equipment shall be via a centralised element manager or equivalent configuration deployment system. For example, Privileged Users shall not be provided with direct access to any management terminal, except where network connectivity is not available (e.g. break-glass situations).

4.89 The Supplier shall ensure that it is not possible to directly communicate between managed elements over the Management Plane.

4.90 The Supplier shall ensure that the Management Plane is segregated by Third Party, and between Access Networks and core networks (e.g. by Virtual LAN). This would not preclude the use of a single orchestration and management solution, provided it is compliant with Paragraph 4.96.

4.91 The Supplier shall ensure that the Management Plane is configured to ensure that only necessary connections are allowed. Specifically, element managers and other administrative functions shall only be able to communicate with the Network Equipment that they administer. Further, Network Equipment shall only be able to communicate with its administrative functions and its ability to establish a connection with these functions shall be limited.

4.92 The Supplier shall ensure that the function authorising Privileged User access (e.g. the root authentication service) is within a trusted security domain (not the corporate network). It shall require Multi-Factor Authentication with credentials being generated outside of the Corporate Security Domain.

4.93 The Supplier shall ensure that Multi-Factor Authentication supporting and authorisation functions is treated as a Network Oversight Function and is within a separate security domain to the Corporate Security Domain.

4.94 The Supplier shall ensure that testing procedures are established and utilised to verify that Management Networks enforce the controls set out in this Management Plane 3 section.

4.95 The Supplier shall ensure that their wider network outside of the Management Plane is continuously scanned to detect and remediate unnecessary open management protocols, ports and services.

4.96 The Supplier shall ensure that the Management Plane is segregated in such a way that a disruption to a segment shall not affect the entirety of the Supplier's UK network.

4.97 The Supplier will ensure they, and their Third Parties, adhere to the following requirements for PAWs:

4.97.1 only have limited internet access and where required shall be via VPN;

4.97.2 only have access to internal-only business systems;

4.97.3 support secure boot, boot attestation & encryption at rest backed by a hardware root-of-trust;

4.97.4 be kept up to date with latest OS patches throughout its lifetime, with security patches being applied within 14 days of release;

4.97.5 shall prevent unauthorised code from executing;

4.97.6 have health attestation capability which is used wherever possible, particularly if located outside the UK;

4.97.7 shall be monitored in real time, and

4.97.8 shall use data-at-rest encryption.

4.98 The Supplier shall ensure that all new deployments of equipment are administered via secure, encrypted and authenticated protocols. The Supplier shall ensure that insecure or proprietary security protocols are disabled.

4.99 The Supplier shall ensure that any exceptions to Paragraph 4.98 above are authorised at the appropriate level within the Supplier's organisation, with the risk posed and mitigation applied

being justified and fully documented and reported at the appropriate level within the Supplier's organisation.

4.100 The Supplier shall ensure that security protocols and algorithms shall not be proprietary whenever technically viable.

4.101 The Supplier shall ensure that each Network Equipment has strong, unique credentials for every account.

4.102 The Supplier shall ensure that any equipment, used to provide the Outsourced Infrastructure, that reaches the Vendor's End-Of-Life Date, the Supplier shall only continue to use the equipment if the following conditions are met:

4.102.1 The equipment's configuration is rarely modified, and modifications are reviewed.

4.102.2 Either the addressable interfaces of the unsupported equipment are monitored and use of those interfaces can be explained, or there is no realistic possibility that exploitation of all unsupported equipment would have an impact on the network.

4.102.3 The network exposure (potential attack surface) of the unsupported equipment is minimal.

Network Oversight Functions Measures

4.103 The Supplier shall ensure that Network Oversight Functions shall be robustly locked-down, in support and patched within such period as is proportionate to the risk of security compromise that the patch is intended to address and as set out in Paragraph 4.75. Should this not be possible, patches shall be deployed on Network Oversight Functions as soon as practicable and robust alternative mitigations put in place until the relevant patch has been deployed.

4.104 The Supplier shall ensure that any service that supports or contains Network Oversight Functions is rebuilt to an up to date, known-good software state every 24 months. This includes the operating system and application software. This can be performed in line with a system upgrade.

4.105 The Supplier shall ensure that any workstations or functions (e.g. Jump Boxes) through which it is possible to make administrative changes to Network Oversight Functions are rebuilt to an up to date, known-good software state every 12 months. This applies to the workstation or function's operating systems and above.

4.106 The Supplier shall run Network Oversight Functions on Trusted Platforms.

4.107 Where the Supplier cannot guarantee the security of the physical environment (e.g. within the Exposed Edge, or within a shared data centre/exchange) Network Oversight Functions shall not be deployed.

4.108 The Supplier shall ensure that Network Oversight Functions are only managed by a minimal set of trusted Privileged Users. All Management Accesses to Network Oversight Functions shall be pre-authorised by a limited set of people who have been assigned with an appropriate role.

4.109 The Supplier will use dedicated management functions (e.g. Jump-Box) to manage Network Oversight Functions that are only accessible from designated PAWs. This Management Network shall be isolated from other internal and external networks, including the Management Network used by other equipment.

4.110 The Supplier shall monitor in real time (e.g. SYSLOG) any changes to Network Oversight Functions with designated PAWs, dedicated management functions and the Network Oversight Functions themselves monitored for signs of exploitation.

4.111 The Supplier shall ensure that Network Oversight Functions only access services (e.g. AAA, network time, software updates) over Internally-Facing Interfaces.

Monitoring and Analysis

4.112 The Supplier shall use appropriately skilled and dedicated resources to understand and analyse security-related network activity.

4.113 The Supplier shall ensure that threat hunting is periodically performed using available logging and monitoring data. If possible, the Supplier should not outsource audit or threat hunting to any party involved in operating the network.

4.114 The Supplier shall keep asset management and network monitoring systems up to date to enable security staff to identify and track down anomalies within networks. This shall include comprehensive details of normal system and traffic behaviour (e.g. source and destination, frequency of communication, protocols and ports used, and expected bandwidth consumed).

4.115 The Supplier shall maintain monitoring processes for assessing, notifying and implementing network changes and modify the processes if necessary.

4.116 The Supplier shall monitor physical and logical interfaces between networks that operate at different Trust Levels, as well as between groups of network functions (e.g. core networks and Access Networks).

4.117 The Supplier shall protect the integrity of logging data and any modification shall be alerted and attributed.

4.118 The Supplier shall make all actions involving stored logging or monitoring data (e.g. copying, deleting, modification or viewing) traceable back to an individual user.

4.119 The Supplier shall keep logging datasets synchronised, using common time sources, so separate datasets can be correlated in different ways.

4.120 The Supplier shall raise an alarm if logs stop being received from any Network Equipment.

4.121 The Supplier shall fully record logs for Network Equipment in Security Critical Functions and retain such logs for 13 months. The Supplier shall make such logs available for audit for 13 months where reasonably required by VMO2.

4.122 The Supplier shall ensure that Network-Based Sensors and Host-Based Sensors are deployed and run throughout networks to obtain traffic to support Security Analysis.

4.123 The Supplier shall collect access events to Network Equipment and consider unauthorised access attempts to be a security event.

4.124 The Supplier shall ensure that logging data is enriched with other network knowledge and data. In order to successfully analyse logging data, it must be used in conjunction with knowledge of the Supplier's network as well as other pertinent data needed for understanding log entries.

4.125 The Supplier shall regularly and automatically collect and audit Network Equipment configurations to detect unexpected changes.

4.126 The Supplier shall keep all logs linked back to specific Network Equipment or services.

4.127 The Supplier shall process and analyse logs in near real-time (in any case within five minutes) and generate security relevant events.

4.128 The Supplier shall ensure that tools and techniques are utilised to support analysts in understanding the data collected.

4.129 The Supplier shall regularly review access logs and correlate this data with other access records and ticketed activity.

4.130 The Supplier shall ensure that indications of potential anomalous activity, and potential malicious activity, are promptly assessed, investigated and addressed.

4.131 The Supplier shall ensure that logging data is correlated with data within asset management systems to detect anomalies. Models shall be developed to characterise 'normal' traffic within networks, including type and volume.

Management Plane Measures 4

4.132 The Supplier shall ensure that:

4.132.1 its administrators do not need Privileged Access to Network Equipment to make administrative changes;

4.132.2 its administrators have Privileged Access to administrative systems (e.g. OSS) which make the necessary changes on the administrator's behalf;

4.132.3 administrative systems group administrative changes to automate administrative processes and minimise administrator input and risk;

4.132.4 when an administrator uses a Privileged Access into a Security Critical Function, which is not an administrative system, this creates a security alert.

Monitoring and Analysis 2

4.133 The Supplier shall ensure that automated tools are used to find and prioritise events that require manual analysis.

Retaining National Resilience and Capability

4.134 The Supplier shall ensure, so far as is reasonably practicable, that the equipment performing the Supplier's Network Oversight Functions is located within the UK, and operated using UK-based staff. Where it is not reasonably practicable to comply with this Paragraph, the Supplier shall inform VMO2 in writing and provide VMO2 with a written risk assessment within thirty (30) days of the relevant Network Oversight Function being implemented and/or operational responsibility being provided from outside the UK.

4.135 The Supplier shall retain a UK-based technical capability to provide subject matter expertise on the operation of the Supplier's UK networks and the risks to the Supplier's UK networks.

4.136 Where VMO2 Information is stored offshore, the Supplier shall maintain a list of locations where the data is held. The risk due to holding the data in these locations, including any risk associated with local data protection law, shall be managed as part of the Supplier's risk management processes.

4.137 Without prejudice to any other Supplier obligations in the Agreement, including any other requirements of the Security Schedule, and any other agreement between VMO2 and the Supplier relating to data processing, the Supplier shall ensure that decisions about holding outside of the UK data relating to more than 100,000 VMO2 subscribers, the operation of the large parts of the network, or the operation of Network Oversight Functions, shall be taken at an appropriate governance level and recorded in writing. The sign-off for these decisions should normally be given by a person or committee at board level (or equivalent). The Supplier shall inform VMO2 promptly of any such decisions.

4.138 If it should become necessary to do so, the Supplier shall have the ability to maintain (as relevant, where it provides such a form of connectivity prior to the event) the following UK network connectivity for a period of one month in the event of loss of international connections: fixed and mobile data connectivity to UK peering points; mobile voice; and text-based mobile messaging.

4.139 If it should become necessary to do so, the Supplier shall be able to transfer into the UK functions required by UK networks to maintain an operational service, should international bearers fail.

Listed Countries

4.140 The Supplier must ensure that any tools (a) are not capable of being accessed from a Listed Country, and (b) are not stored on equipment located in a Listed Country. Tools shall cover tools that enable (a) the monitoring or analysis in real time of the use or operation of the network or service, or (b) the monitoring or analysis of the content of signals (Regulation 5(3)).

4.141 The Supplier must ensure that (a) no Security Permission is given to a person while the person is in a Listed Country, and (b) any Security Permission cannot be exercised while the person to whom it is given is in a Listed Country (Regulation 8(6)).

4.142 The Supplier shall ensure that contingency procedures are in place in the event that further locations are added to the schedule of Listed Countries in the Regulation.

5. MEASURES APPLICABLE TO OUTSOURCED INFRASTRUCTURE SUPPLIERS THAT UTILISE VIRTUALISATION SERVICES

Virtualisation Measures 1

5.1 The Supplier shall ensure that the Virtualisation Fabric is robustly locked down, uses the latest patch for the software version and is in support.

5.2 The Supplier shall ensure that it is possible to update the Virtualisation Fabric without negatively impacting the network functionality.

5.3 The Supplier shall ensure that:

5.3.1 all interfaces on physical hosts are locked down to restrict access

5.3.2 the only incoming connection to the physical host is for management purposes or to support the virtualisation function

5.3.3 there are no outgoing connections except to support virtual workloads. Communication between physical hosts shall be inhibited other than as part of data flows between virtual workloads

5.3.4 communication between physical hosts is inhibited other than as part of data flows between virtual workloads.

5.4 The Supplier shall ensure that controls are in place to ensure that only known physical hosts can be added to the Virtualisation Fabric.

5.5 The Supplier shall ensure that any modification of databases and systems that define the operation of the network is signed off by two authorised persons.

5.6 The Supplier shall ensure that, as part of the Virtualisation Fabric, physical separate ports are used to segregate internal interface and external interface network traffic.

5.7 The Supplier shall ensure that the Virtualisation Fabric is configured to limit the exposure of virtual workloads (e.g. disable virtual span ports by default).

5.8 The Supplier shall ensure that the Virtualisation Fabric is configured to prevent use of hard-coded MAC addresses by default (e.g. by individual VNFs).

5.9 The Supplier shall ensure that the Virtualisation Fabric is configured to encrypt data at rest (including no data to be written to the host's storage unencrypted and data to be encrypted when the host is powered off).

5.10 The Supplier shall ensure that where there is risk of exposure during transmission, the Virtualisation Fabric is configured to securely encrypt data in transit. Examples and guidance on the use of encryption can be found on the NCSC website (Using TLS to protect data (NCSC, 2021) https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data).

5.11 The Supplier shall ensure that all physical hosts shall be placed into a host security 'pool'. Pools may be defined based on the environment within which that host resides, the type of host, resilience and diversity, purpose etc.

5.12 The Supplier shall ensure that virtual workloads shall be authorised, tagged with a specific trust domain, and signed prior to use. The specific trust domain shall be based on the risks associated with the workload.

5.13 The Supplier shall ensure that there is separation between trust domains. This separation may be enforced by the Virtualisation Fabric, provided Virtualisation Cut-Throughs are not used.

5.14 The Supplier shall ensure that host pools are tagged with trust domains they can execute. This will be based on risk and ensure that sensitive functions are not executed alongside vulnerable functions, or in physically exposed locations. The Virtualisation Fabric shall verify that the virtual workload is signed and complies with policy prior to use, including that the virtual workload's trust domain is permitted to execute within the host's pool.

5.15 The Supplier shall ensure that a physical host shall not be able to impact hosts in other host pools. This includes, but is not limited to, spoofing Virtual LAN/Virtual Extensible LANs of virtual networks.

5.16 The Supplier shall ensure that Containers are not used to implement separation between trust domains. To implement separation between trust domains, the Supplier shall use Bare Metal Hypervisors (without Virtualisation Cut-Throughs) or discrete physical hardware.

5.17 The Supplier shall ensure that Containerised hosts shall only support a single trust domain.

5.18 The Supplier shall ensure that control and orchestration functions for virtualisation are Network Oversight Functions and reside in a trusted physical and logical location.

5.19 The Supplier shall ensure that the administration network of the Virtualisation Fabric is a Management Plane and protected as such.

5.20 The Supplier shall ensure that Privileged Access to the Virtualisation Fabric is only available over authenticated and encrypted channels.

5.21 The Supplier shall ensure that functions that support the administration and security of the Virtualisation Fabric do not run on the fabric they are administering.

5.22 The Supplier shall ensure that functions that support the administration and security of the Virtualisation Fabric are Network Oversight Functions and shall reside in a trusted physical and logical location.

5.23 The Supplier shall ensure that the number of privileged accounts for the Virtualisation Fabric is constrained to the minimum necessary to meet the Supplier's needs.

5.24 The Supplier shall ensure that the Virtualisation Fabric administrator accounts do not have any privileged rights to other services within the Supplier, or vice-versa.

5.25 The Supplier shall ensure that the Virtualisation Fabric administrator accounts are only provided with the privileges and accesses required to carry out their role.

5.26 The Supplier shall ensure that the Virtualisation Fabric administrator accounts do not have access to the Supplier's workloads running within the virtualised environment.

5.27 The Supplier shall ensure that the Network Oversight Functions do not share trust domains or host pools with workloads that are not Network Oversight Functions.

5.28 The Supplier shall ensure that Containers are not used to enforce separation between different Network Oversight Functions and between Network Oversight Functions and other functions.

Virtualisation 2

5.29 The Supplier shall ensure that all non-ephemeral secrets, passwords and keys shall be stored in hardware-backed secure storage. Where the Supplier is not able to apply this measure to existing Services, the Supplier must set out in writing (including consulting with VMO2) what mitigating steps they are taking within thirty (30) days.

5.30 The Supplier shall ensure that only physical hosts that have been Cryptographically Attested to be in a known-good state can be provisioned into the Virtualisation Fabric.

5.31 The Supplier shall ensure that where the Virtualisation Fabric allows virtual functions to have direct access to the physical hardware (Virtualisation Cut-Throughs), it is not treated as a security boundary.

5.32 The Supplier shall ensure that where possible, the Virtualisation Fabric is built and updated through an automated and verifiable process.

5.33 The Supplier shall ensure that where possible, only automated and verifiable methods of configuration are used for administration of the Virtualisation Fabric (authorised API calls etc).

5.34 The Supplier shall ensure that where possible, administration of the Virtualisation Fabric is automated during normal operation.

5.35 The Supplier shall ensure that manual administration of the Virtualisation Fabric (e.g. access to a command line on host infrastructure) produces an immediate alert.

6. MEASURES APPLICABLE TO OUTSOURCED INFRASTRUCTURE SUPPLIERS THAT UTILISE NETWORK SIGNALLING SERVICES

6.1 The Supplier shall understand how incoming signalling arrives into their network, and outgoing signalling leaves their network. Specifically, this includes an understanding of the interfaces over which signalling enters and leaves the network, and the equipment which sends and processes external signalling.

6.2 The Supplier shall have an appropriate understanding of (i) what Network Equipment could be impacted by malicious signalling and (ii) what Network and User Data could be compromised through malicious signalling. The Supplier shall understand who they directly connect with over the signalling network and operate on the principle that Incoming Signals are from untrusted networks.

6.3 The Supplier shall ensure that, at edge signalling nodes, any incoming messages using any source address internal to the Supplier's network are blocked.

6.4 The Supplier shall ensure that trust is not assumed based on the source of any incoming message for example, 'UK' source addresses (e.g. +44 global titles in SS7) shall not be assumed to be trusted and shall not be allowed by default.

6.5 The Supplier shall ensure that where the signalling message is protected by end-to-end authentication, risk decisions and associated security controls may be determined based upon the authenticated source.

6.6 Where the Supplier allows others to use number ranges that have been allocated to them (e.g. GTs, IMSIs), the Supplier shall ensure they remain responsible for the activity related to that number range, and any further security implications. This does not apply in the case of MSISDNs shared through MNP.

6.7 The Supplier shall ensure that any outgoing message that uses a source address that should not transit or leave the Supplier's network shall not be permitted to leave the Supplier's network.

6.8 The Supplier shall ensure that their network shall only send outgoing signalling in support of services permitted by the recipient. Guidance on what the GSMA has defined as permitted services is set out within Section 5 of GSMA's charging and accounting principles and Section 10 of GSMA's interconnection and interworking charging principles.

6.9 The Supplier shall ensure that external BGP (border gateway protocol) updates are monitored for evidence of misuse and upon discovery of any misuse that impacts VMO2, the Supplier shall notify VMO2 promptly (but by no later than 48 hours) in writing via email to security.incident@virginmediao2.co.uk of becoming aware of any such misuse.

6.10 The Supplier shall mitigate any BGP misuse that impacts the Supplier's network and/or services in a timely manner, and at least within 12 hours whenever technically possible.

6.11 The Supplier shall ensure that contact details are current and accurate on all the Regional Internet Registries (e.g. RIPE) and shall endeavour to keep other data sources accurate.

6.12 The Supplier shall ensure that all address space and autonomous system number (ASN) resources allocated to the Supplier shall be correctly recorded in such a way that it is simple to identify and contact the 'owner' to assist in resolving issues.

6.13 The Supplier shall implement ingress and egress route filtering.

6.14 The Supplier shall adopt and implement mechanisms that prevent IP address spoofing.

6.15 The Supplier shall share such details in writing, as are appropriate and proportionate, of any BGP misuse with VMO2 promptly (but by no later than 48 hours) where it may cause a Security Compromise.

6.16 The Supplier shall ensure that an external path update that includes a prefix owned by the Supplier is not accepted.

6.17 The Supplier shall ensure that end-users are not able to spoof IPs over the data plane e.g. in line with BCP38.

6.18 The Supplier shall ensure that any incoming or outgoing message type that should not be sent over international or external signalling networks are blocked at the Logical Edge of the Network. For example, GSMA CAT 1 messages shall be blocked for SS7 networks, and equivalent messages shall be blocked for other signalling protocols such as Diameter, GTP, Interconnect and SS7/SIGTRAN.

6.19 The Supplier shall ensure that, when sent over signalling networks, the external exposure of customer data, customer identifiers and network topology information shall be minimised.

6.20 The Supplier shall have in place the means for recipients of their BGP routing updates to validate that the BGP routing update originated from the legitimate owner.

6.21 The Supplier shall, where the necessary information is available, validate that any BGP route updates they receive have originated from the legitimate owner.

6.22 The Supplier shall monitor incoming and outgoing signalling traffic.

6.23 Signalling records are Sensitive Data and the Supplier shall protect such records from misuse or extraction.

6.24 The Supplier shall perform Security Analysis on signalling traffic to find and address anomalous signalling and malicious signalling.

6.25 The Supplier shall establish an effective means to alert VMO2 to malicious signalling where there could be a Security Compromise.

6.26 The Supplier shall perform detailed Negative Testing and Fuzzing for all interfaces that process data provided over an external signalling interface (including existing equipment). The Supplier shall test that the live configuration prevents malformed, inconsistent, unexpected, or abnormally high volumes of signalling messages from disrupting Security Critical Functions.

6.27 The Supplier shall ensure that their critical, core and signalling security systems are highly resilient to signalling attacks. Signalling messages shall be validated at the Logical Edge of the Network prior to being forwarded to critical or Core Nodes. Messages that are not encoded in a normal manner, or that are unrelated to a normal operation or call flow in the network, shall be blocked. All exceptions to this shall be understood, justified, and documented.

6.28 The Supplier shall ensure that a signalling failure for an Externally-Facing Service shall not impact Core Nodes or Security Critical Functions.

6.29 The Supplier shall ensure that, with the exception of SS7 and GTP-C, only 'hub' signalling addresses shall be exposed externally. This shall be done in such a way that internal signalling addresses of critical Core Nodes are not shared or exposed externally.

6.30 The Supplier shall ensure that outgoing signalling shall be authenticated where this is supported by international standards.

6.31 The Supplier shall ensure that customer data and customer identifiers shall be obfuscated before being released over an external signalling network, except where it is functionally essential to provide this information.

6.32 The Supplier shall ensure that in protocols other than SS7 and GTP-C, signalling network topology information shall be obfuscated before being released over an external signalling network, except where it is functionally essential to provide this information.

7. MEASURES APPLICABLE TO OUTSOURCED INFRASTRUCTURE SUPPLIERS THAT PROVIDE, INSTALL AND CONFIGURE CUSTOMER PREMISE EQUIPMENT

7.1 Once the CPE has been configured at the customer site, the Supplier shall ensure that the CPE only contain credentials that are both unique to that CPE, and not guessable from CPE metadata.

7.2 The Supplier shall ensure that all CPE provided to VMO2 customers remains supported by the Network Equipment supplier or if the CPE goes out of Supplier support, the Supplier shall inform

VMO2 in advance and proactively offer a suitable replacement at no additional cost to VMO2 as soon as reasonably practicable and in any event before the CPE is out of support.

7.3 The Supplier shall ensure that Wide Area Network CPE management interfaces shall only be accessible from specified management locations (e.g. URL or IP address).

7.4 The Supplier shall ensure that management of the CPE shall use a secure protocol (e.g. TLS 1.2 or newer).

7.5 The Supplier shall ensure that, by default, the CPE's customer-facing management interfaces shall only be accessible from within the customer's network.

7.6 The Supplier shall ensure that, by default, all unsolicited incoming connections towards the customer's network shall be blocked by the CPE.

ANNEX TO APPENDIX B, PART 2: CODE OF PRACTICE AND APPENDIX REFERENCING

Code of Practice measure number	Corresponding Appendix Paragraph	Code of Practice measure number	Corresponding Appendix Paragraph	Code of Practice measure number	Corresponding Appendix Paragraph
M1.01	4.1	M10.19	4.51	M13.07	5.7
M1.02	4.2	M10.20	4.52	M13.08	5.8
M1.03	4.3	M10.21	4.53	M13.09	5.9
M1.04	4.4	M10.22	4.54	M13.10	5.10
M1.05	4.5	M10.23	4.55	M13.11	5.11
M1.06	4.6	M10.24	4.56	M13.12	5.12
M2.01	4.7	M10.25	4.56	M13.13	5.13
M2.02	4.8	M10.26	4.56	M13.14	5.14
M2.03	4.8	M10.28	4.56	M13.15	5.15
M2.04	4.9	M10.29	4.56	M13.16	5.16
M2.05	4.10	M10.30	4.56	M13.17	5.17
M2.06	4.11	M10.31	4.57	M13.18	5.18
M3.01	6.1	M10.32	4.58	M13.19	5.19
M3.02	6.2	M10.33	4.59	M13.20	5.20
M3.03	6.2	M10.34	4.60	M13.21	5.21
M3.04	6.2	M10.35	4.61	M13.22	5.22
M3.05	6.3	M10.36	4.62	M13.23	5.23
M3.06	6.4	M10.37	4.62	M13.24	5.24
M3.07	6.5	M10.38	4.62	M13.25	5.25
M3.08	6.6	M10.39	4.63	M13.26	5.26
M3.09	6.7	M10.40	4.64	M13.27	5.27
M3.10	6.8	M10.41	4.64	M13.28	5.28
M3.11	6.9	M10.42	4.65	M14.01	4.102
M3.12	6.10	M10.43	4.66	M15.01	4.103
M3.13	6.11	M10.44	4.67	M15.02	4.104

M3.14	6.12	M10.45	4.68	M15.03	4.105
M3.15	6.13	M10.46	4.69	M15.04	4.106
M3.16	6.14	M10.47	4.70	M15.05	4.107
M3.17	6.15	M10.48	4.71	M15.06	4.108
M3.18	6.16	M10.49	4.72	M15.07	4.109
M3.19	6.17	M10.50	4.73	M15.08	4.109
M4.01	4.12	M10.51	4.74	M15.09	4.109
M4.02	4.12	M10.52	4.75	M15.10	4.108
M4.03	4.13	M10.53	4.76	M15.11	4.110
M4.04	4.14	M10.54	4.77	M15.12	4.110
M4.05	4.15	M11.01	4.78	M15.13	4.111
M5.01	4.16	M11.02	4.79	M16.01	4.112
M5.02	4.17	M11.03	4.80	M16.02	4.113
M5.03	4.18	M11.04	4.81	M16.03	4.113
M5.04	4.19	M11.05	4.81	M16.04	4.114
M5.05	4.20	M11.06	4.81	M16.05	4.115
M5.07	4.21	M11.07	4.81	M16.06	4.116
M6.01	4.22	M11.08	4.82	M16.08	4.117
M6.02	4.23	M11.09	4.83	M16.09	4.118
M6.03	4.24	M11.10	4.84	M16.10	4.119
M6.04	4.25	M11.11	4.85	M16.11	4.120
M6.05	4.26	M11.12	4.85	M16.12	4.121
M7.01	6.18	M11.13	4.86	M16.13	4.122
M7.02	6.19	M11.14	4.87	M16.14	4.123
M7.03	6.20	M11.15	4.88	M16.15	4.124
M7.04	6.21	M11.16	4.89	M16.16	4.125
M8.01	4.27	M11.17	4.90	M16.17	4.126
M8.03	4.28	M11.18	4.91	M16.18	4.127

M8.05	4.29	M11.19	4.92	M16.19	4.128
M8.06	4.30	M11.20	4.93	M16.20	4.129
M8.07	4.31	M11.21	4.94	M16.21	4.130
M8.08	4.32	M11.22	4.95	M16.22	4.131
M9.01	7.1	M11.23	4.96	M17.01	4.132
M9.02	7.2	M11.24	4.97	M18.01	6.27
M9.03	7.3	M11.25	4.97	M18.02	6.28
M9.04	7.4	M11.26	4.97	M18.03	6.29
M9.05	7.5	M11.27	4.97	M18.04	6.30
M9.06	7.6	M11.28	4.97	M18.05	6.31
M10.01	4.33	M11.29	4.97	M18.06	6.32
M10.02	4.34	M11.30	4.97	M19.01	5.29
M10.03	4.35	M11.31	4.97	M19.02	5.30
M10.04	4.36	M11.32	4.98	M19.03	5.31
M10.05	4.37	M11.33	4.99	M19.04	5.32
M10.06	4.38	M11.34	4.100	M19.05	5.33
M10.07	4.39	M11.35	4.101	M19.06	5.34
M10.08	4.40	M12.01	6.22	M19.07	5.35
M10.09	4.41	M12.02	6.23	M20.01	4.133
M10.10	4.42	M12.03	6.24	M21.01	4.142
M10.11	4.43	M12.04	6.25	M21.02	4.134
M10.12	4.44	M12.05	6.26	M21.03	4.135
M10.13	4.45	M13.01	5.1	M21.04	4.136
M10.14	4.46	M13.02	5.2	M21.05	4.137
M10.15	4.47	M13.03	5.3	M21.06	4.138
M10.16	4.48	M13.04	5.4	M21.07	4.139
M10.17	4.49	M13.05	5.5		
M10.18	4.50	M13.06	5.6		