Virgin Media O2 Security Schedule

Contents

Purpose and Scope 3

Definitions 3

1.0 Information Security 4

2.0 Detection 5

3.0 Legal & Regulatory Compliance 6

4.0 Compliance 6

5.0 Breaches and Compliance Failures 7

6.0 Retention of VMO2 Information 8

7.0 Access Control 8

8.0 Business Continuity 9

9.0 Physical Security 10

10.0 Human Resource Security 11

11.0 Audit 11

12.0 Portable Device Security 12

13.0 Backup 13

14.0 Vulnerability Management 14

15.0 Logging & Monitoring 16

16.0 Fourth Parties 16

17.0 Cloud Security 16

Appendix A – additional legal, regulatory and contractual requirements 19

1.0 Payment Card Industry Data Security Standard (PCI DSS) 19

2.0 Sarbanes Oxley Compliance 19

3.0 Network and Information Systems Regulations (NIS) 2018 19

4.0 Smart Metering 20

5.0 Resilience Controls 20

6.0 Telecommunications Security Act 2021 20

1.0 Purpose 21

2.0 Controls applicable to all TSA vendors 22

3.0 Controls applicable to specific TSA vendors 23

3.1 Controls applicable to vendors who provide third party administrative support (3PA) 23

3.2 Controls applicable to all vendors who provide network equipment (both software and/or hardware) 25

3.3 Controls applicable to SIM manufacturers 26

3.4 Controls applicable to vendors who provide customer premise equipment 27

3.5 Controls applicable to vendors who provide an externally hosted or managed network oversight function 27
3.6 Controls applicable to vendors who provide deliver & configure services 29
3.7 Controls applicable to vendors who provide externally hosted infrastructure 29

Purpose and Scope

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.

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. The term "VMO2" in this Schedule refers to any member of Virgin Group who is a recipient of the services, equipment, and software provided by the Supplier or third parties.

Definitions

For the purposes of this Schedule:

"**Agreement**" refers to the agreement which attaches this Schedule as an appendix or schedule or refers to this Schedule and is between the third party referred to at the start of the agreement (the "**Supplier**") and 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.

"**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 including any Cloud Based Services provided by the Supplier pursuant to the Agreement.

"**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.

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

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.

"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.

"Fourth Party" 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 Parties 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.

1.0 Information Security

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

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

1.3 The Supplier shall advise VMO2 or their agents of any areas of non-compliance with VMO2 security requirements stated within this Schedule.

1.4 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 Schedule.

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

1.6 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 4.2) or the right to audit (section 11.0).

1.7 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.

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

1.9 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.

1.10 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.

1.11 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.

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

1.13 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.

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

1.15 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.

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

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

1.18 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).

1.19 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).

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

1.21 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.).

2.0 Detection

2.1 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.

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

2.3 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.

3.0 Legal & Regulatory Compliance

3.1 Without prejudice to any other rights or remedies VMO2 may have, any material or persistent breach of this 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).

3.2 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.

3.3 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.

3.4 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.

3.5 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 5.2 below.

3.6 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.

3.7 Additional legal and regulatory requirements are detailed in Appendix A to this 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

6.0 Telecommunications (Security) Act 2021

4.0 Compliance

4.1 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.

4.2 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 11.0 below.

4.3 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 Schedule within 30 days of notice to the Supplier.

5.0 Breaches and Compliance Failures

5.1 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 5.2.

5.2 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.

5.3 With the exception of data breaches, which shall be notified in accordance with paragraph 5.2 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.

5.4 Notifications required in this section 5.0 shall be notified by the Supplier to VMO2 by emailing security.incident@virginmediao2.co.uk

5.5 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 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 Schedule.

5.6 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 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.

5.7 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.

6.0 Retention of VMO2 Information

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

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

6.3 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

6.4 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.

6.5 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:

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

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

6.6 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.

6.7 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.

7.0 Access Control

7.1 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.

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

7.3 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.

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

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

7.6 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.

7.7 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.

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

7.9 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.

7.10 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.

7.11 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.

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

7.13 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).

7.14 Multi-factor authentication is required for remote access.

7.15 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.

7.16 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.

8.0 Business Continuity

8.1 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.

8.2 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.

8.3 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.

8.4 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.

9.0 Physical Security

9.1 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.

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

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

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

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

9.3.3 the electronic access control system should be appropriately maintained.

9.4 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.

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

9.6 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.

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

9.8 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.

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

9.10 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.

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

10.0 Human Resource Security

10.1 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.

10.2 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.

10.3 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.

10.4 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.

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

10.6 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.

10.7 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.

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

11.0 Audit

11.1 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. The purpose of this audit is to inspect and verify the compliance of the Supplier with its obligations under this 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 Suppliers obligations under this Schedule. For the avoidance of

doubt, completion of the information security questionnaire shall not be considered an audit pursuant to this paragraph.

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

11.3 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.

11.4 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 Schedule.

11.5 The Supplier shall, without delay, provide reasonable assistance and co-operation with VMO2 in implementing any measures required to correct any non-compliance with Supplier's obligations set out in this Schedule, as detected in any audits carried out pursuant to this Section 11.0.

12.0 Portable Device Security

12.1 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).

12.2 The device security shall ensure that:

12.2.1 temporary storage areas are encrypted;

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

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

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

12.2.5 the passphrase used shall adhere to Good Industry Practice.

12.3 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.

12.4 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.

12.5 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.

12.6 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

12.7 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.

13.0 Backup

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

13.2 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:

- Databases
- Operating/ business systems
- Configuration files and system-level information (including network elements such as routers, switches, firewalls etc.)
- Firmware
- Applications
- Virtualised infrastructure
- User-level data contained in the systems
- Critical documentation including security related documentation

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

13.4 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.

13.5 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.

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

13.7 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.

13.8 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.

13.9 Where systems are in-scope of The Telecoms Security Act, (TSA) (as defined in the TSA Supplier Security Appendix, the Supplier shall maintain read-only backups of their infrastructure and information and shall be able to restore them and be maintained to protect against any accidental or deliberate erasure of data. The backups shall contain the information necessary to maintain the normal operation of the public electronic communications network or public electronic communications service.

14.0 Vulnerability Management

14.1 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.

14.2 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)

14.3 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

14.4 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.

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

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

14.7 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 14.2.

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

14.9 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.

14.10 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.

14.11 The Supplier shall treat any "end of life" or "end of support" notification as a critical vulnerability and react accordingly.

14.12 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.

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

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

14.15 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.

15.0 Logging & Monitoring

15.1 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.

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

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

15.4 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.

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

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

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

16.0 Fourth Parties

16.1 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.

16.2 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.

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

16.4 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.

17.0 Cloud Security

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

17.2 The Supplier must document and implement clearly defined processes for acquisition, use,

management and exit from Cloud Based Services.

17.3 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

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

17.5 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).

17.6 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.

17.7 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.

17.8 The Supplier will implement the following access measures:

a. appropriate levels of account privilege and have authorisation mechanisms in place to enforce the separation of privileges between different types of account.
b. role-based access control to ensure that users only have access to the resources necessary for their role and that these are regularly reviewed.

17.9 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.

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

17.11 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.

17.12 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.

17.13 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.

17.14 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.

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

17.16 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 – additional legal, regulatory and contractual requirements

1.0 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.

2.0 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.

3.0 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.

4.0 Smart Metering

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

5.0 Resilience Controls

If the Supplier is TSA applicable, then this section can be discarded, this section has been created where resilience controls are applicable for non-TSA applicable Suppliers.

5.1 For any agreements with VMO2, the Supplier must do an appropriate resilience risk assessment and disclose it to VMO2.

5.2 The Supplier must recognise and minimise the dangers of security breaches in the VMO2 's network or services brought on 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/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 provider shall work with the third-party supplier to ensure the issue is mitigated until resolved.

5.7 The Supplier will ensure all VMO2 data 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 the data 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 the provider's network or service or to sensitive data.

5.10 The Supplier will make sure 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 give a sense of the scale of this testing.

6.0 Telecommunications Security Act 2021

See document on following page.

VMO2 TSA Supplier Security Appendix

Contents

1.0 Purpose

2.0 Controls applicable to all TSA vendors

3.0 Controls applicable to specific TSA vendors

- 3.1 Controls applicable to vendors who provide third party administrative support (3PA)
- 3.2 Controls applicable to all vendors who provide network equipment (both software or hardware)
- 3.3 Controls applicable to SIM manufacturers
- 3.4 Controls applicable to vendors who provide customer premise equipment (both residential and business)
- 3.5 Controls applicable to vendors who provide an externally hosted and managed network oversight function (e.g. element management solution)
- 3.6 Controls applicable to vendors who provide deliver & configure services
- 3.7 Controls applicable to vendors who provide externally hosted infrastructure

1.0 Purpose

This TSA Supplier Security Appendix identifies additional security requirements for Suppliers whose products or services are used by VMO2 in the delivery of its public electronic communications network or services.

If a Supplier (including a Supplier's supply chain) provides products or services to VMO2 which are in scope for the Telecommunications (Security) Act 2021 (the "**TSA**") then the Supplier must be able to demonstrate adherence to the requirements below. In the event of a conflict between these requirements, the Security Schedule or any other security requirements that VMO2 may have specified, then the most stringent requirement shall be applied.

These requirements reflect the latest guidance from the UK's National Cyber Security Centre (NCSC) and OFCOM (Code of Practice December 2022).

The requirements within this document have staggered dates when they become effective. These have been outlined within the respective categories below.

This Appendix shall be interpreted with reference to the defined terms set out in the TSA including any regulations, code of practice or guidance made pursuant to the TSA.

The Supplier shall be responsible for all Third Parties' compliance, and shall ensure all such Third Parties are compliant, with any applicable controls in this TSA Supplier Security Appendix. For the avoidance of doubt, Third Parties (as defined in the Definitions section in the VMO2 Security Schedule) shall include any OEMs involved in the provision of products and services to VMO2 .

2.0 Controls applicable to all TSA vendors

For existing agreements signed before 31 March 2024, these controls are effective from 31st March 2027

For new agreements signed on or after 31st March 2024, these controls are effective from 1st April 2024 or the signature date of the agreement, whichever is the latter

2.1 The Supplier shall maintain records of all third parties and/or subcontractor details and the major components which are used in the provision of Services (as defined in the Security Schedule) for VMO2.

2.2 The Supplier will complete a VMO2 Shared Responsibility Matrix to be supplied by VMO2 detailing the responsibilities between VMO2, the Supplier and the Supplier's third parties.

2.3 The Supplier shall provide a point of contact for incident management for support/escalation of incidents.

2.4 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, as defined in the Telecommunications Security Act 2021, section 105A(2), as amended and updated or replaced from time to time (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.

2.5 The Supplier shall find and report on the root cause of any security incident that could result in a Security Compromise in the UK within 30 days and rectify any security failings found within a reasonable timeframe. If the Supplier does not resolve any security failings within a reasonable timeframe, VMO2 shall be entitled to terminate the Agreement without penalty.

2.6 Without prejudice to Section 11 of the Security Schedule, the Supplier shall support, as far as appropriate, any security audits, assessments or testing required by VMO2 in relation to the security of the VMO2 network, including those necessary to evaluate the security requirements of this TSA Supplier Security Schedule.

2.7 For any agreements with VMO2, the Supplier must do an appropriate resilience risk assessment and disclose it to VMO2.

2.8 The Supplier must recognise and minimise the dangers of security breaches in the VMO2 's network or services brought on by the Supplier's services or facilities.

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

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

2.11 The Supplier will make sure that network and service security is preserved throughout the termination and changeover of the contract with VMO2.

2.12 The Supplier must state whether fuzz testing is performed and gives a sense of the scale of this testing.

2.13 The Supplier acknowledges VMO2's right to share details of Security Compromises arising from acts or omissions of the Supplier, with the relevant authorities to help identify and reduce risks.

2.14 The Supplier must provide to VMO2 a 'security declaration', signed off by an authorised representative of the Supplier that explains how they maintain their equipment's security throughout its lifetime and record any differences in process across product line. It is a requirement that any such declaration should cover all aspects described within Annex B of the TSA.

2.15 The Supplier will provide details (product and version) of major third-party components and dependencies, including open-source components and the period and level of support.

2.16 The Supplier will support all equipment and all software and hardware subcomponents for the term of the Agreement. The period of support of both hardware and software shall be written into the Agreement.

2.17 The Supplier shall remediate any security issue that poses a security risk on the VMO2 network discovered within the 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.

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

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

2.20 The Supplier must provide a recommended up-to-date secure configuration of any network equipment or service it is providing to VMO2.

3.0 Controls applicable to specific TSA vendors

In addition to the controls set out in Section 2.0 above, the controls set out in this Section 3.0 will apply to the vendors described below.

3.1 Controls applicable to vendors who provide third party administrative support (3PA)

For existing agreements signed before 31 March 2024, these controls are effective from 31st March 2027

For new agreements signed on or after 31st March 2024, these controls are effective from 1st April 2024 or the signature date of the agreement, whichever is the latter

3.1.1 The Supplier shall maintain an up-to-date list of all administrator personnel that are able to access VMO2's network, including their roles, responsibilities and expected

frequency of access. VMO2 reserves the right to request addition, modification and/or removal of these accounts at any time.

3.1.2 The Supplier must ensure any administrative function they manage on behalf of VMO2:

3.1.2.1 is segregated from any other network they may perform similar functions for (e.g., another operator network);

3.1.2.2 uses logically independent privileged access workstations and independent administrative domains and accounts unique to VMO2.

3.1.3 The Supplier shall implement logical separation within the 3PA network to segregate customer data and networks and implement and enforce security functions at the boundary between the 3PA network and VMO2's network.

3.1.4 The Supplier shall share with VMO2 any logs related to VMO2 network access on request.

3.1.5 The Supplier shall monitor and audit the activities of the Supplier personnel when accessing the VMO2 network.

3.1.6 The Supplier shall agree to participate in regular testing as VMO2 applies to themselves (e.g., TBEST testing as set for the provider by Ofcom from time to time).

3.1.7 Where the Supplier requires a third party to support the VMO2 network, they shall not transfer control or data pertaining to the network without prior written consent by VMO2.

3.1.8 The Supplier will only access VMO2's network via mediation points owned and operated by VMO2. Where the Supplier requires a third party to support the VMO2 network, this will not be before prior written consent of VMO2.

3.1.9 The Supplier shall ensure that VMO2 network access required for administrative support shall be limited to the minimum required to perform its contractual functions as set out in the Agreement.

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

3.1.11 When the administrator has access to the provider's network or service or to sensitive data, the Supplier shall ensure that any administrator controls they apply are at least as rigorous as the VMO2 controls set out in TSA supplier Security Appendix, the Security Schedule and those set out in the RFP/bid documentation provided by VMO2.

Effective from 31st March 2027

3.1.12 Where relevant, the Supplier shall appropriately protect any persistent credentials that are used for emergency scenarios such as break-glass access. The storage of these credentials shall be encrypted and use secure boot that can only be leveraged within protected environments.

3.1.13 Where the Supplier requires privileged access into the VMO2 network, they shall provide their own Privileged Access Workstations (PAW) to carry out such access. The Supplier will ensure they adhere to following requirements for their provided PAWs:

- Only have limited internet access and where required shall be via VPN;
- Only have access to internal-only business systems;
- Have secure boot, boot attestation & encryption at rest capabilities;
- Be kept up to date with latest OS patches throughout its lifetime, with security patches being applied within 14 days of release;
- Shall prevent unauthorised code from executing;
- Have health attestation capability, particularly if located outside the UK, and
- Shall be monitored in real time.

3.1.14 The Supplier will inform VMO2 whenever administrative access is not possible via defined, secure channels, to reduce the risk posed by such use.

3.1.15 The Supplier will not use proprietary security protocols and algorithms whenever technically viable.

3.1.16 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.

3.2 Controls applicable to all vendors who provide network equipment (both software and/or hardware)

Effective from 31st March 2024

3.2.1 Where the Supplier provides network equipment, appropriate steps shall be taken to prevent IP spoofing by either the end user or an unknown party.

For existing agreements signed before 31 March 2024, these controls are effective from 31st March 2027

For new agreements signed on or after 31st March 2024, these controls are effective from 1st April 2024 or the signature date of the agreement, whichever is the latter

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

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

Effective from 31st March 2025

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

3.2.5 During the procurement of equipment, prior to contract award, the Supplier shall ensure that the security functionality of all equipment has been tested, including using negative testing and fuzzing of equipment interfaces and provide evidence of such testing to VMO2 on request from VMO2. Any third party testing in relation to the security of the equipment shall only be accepted as evidence by VMO2 if it is repeatable, performed independently of the network equipment supplier and is clearly applicable to VMO2's deployment (e.g. relates to the hardware, software and configuration that is being supplied).

3.2.6 Where the Supplier has not complied with Paragraph 3.2.5 (including for the avoidance of doubt if there are any non-compliances with the testing requirements), VMO2 may, without prejudice to any other rights or remedies VMO2 may have, in its discretion choose to carry out such testing themselves, and the Supplier shall pay the cost of such testing or VMO2 shall have the right to terminate in whole or part the Agreement or statement of work (where applicable) without any liability to the Supplier.

Effective from 31st March 2027

3.2.7 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 VMO2's management plane.

3.3 Controls applicable to SIM manufacturers

Effective from 31st March 2024

3.3.1 Where the Supplier provides fixed-profile SIM cards to VMO2, on request from VMO2, the Supplier shall demonstrate that SIM cards are independently audited. through the GSMAs SAS Scheme.

3.4 Controls applicable to vendors who provide customer premise equipment

Effective from 31st March 2025

3.4.1 Where the Supplier provides products or services relating to CPE, the Supplier shall ensure that it does not contain credentials that are default or guessable from CPE metadata, and only contains credentials that are unique to that CPE and management of the CPE interfaces is only accessible from specified locations (e.g., URL/IP address).

3.4.2 Where the Supplier provides products or services relating to CPE, the Supplier shall ensure the CPE is configured to use a secure protocol (e.g., TLS 1.2 or above) and blocks any unsolicited traffic from customer networks. all unsolicited incoming connections towards the customer's network shall be blocked by the CPE.

3.5 Controls applicable to vendors who provide an externally hosted or managed network oversight function

Effective from 31st March 2027

3.5.1 The Supplier must appropriately design and segregate network oversight functions (NOFs), which 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 (OSS)

3.5.2 NOFs must be securely housed and operated on trusted platforms from other parts of VMO2's or Supplier's network. NOFs shall be robustly locked-down, in support and

patched within such period as is appropriate in the circumstances, having regard to the severity of the risk of a Security Compromise which the patch or mitigation addresses.The Supplier must ensure that any service that supports or contains a network oversight functions shall be rebuilt to an up todate, known-good software state every 24 months. This includes the operating system and application software.

3.5.3 The Supplier must ensure that any workstations or functions (e.g. jump boxes) through which it is possible to make administrative changes to network oversight functions shall be rebuilt to an up to date, known-good software state every 12 months

3.5.4 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.

3.5.5 The Supplier will ensure privileged access to virtualisation infrastructure:

- is only be via authenticated and encrypted channels;
- constrains the accounts required to the minimum necessary;
- ensures administrators do not have any privileged rights to other services within the VMO2;
- ensure administrators only have the privilege and access required to carry out their function, and
- ensure administrator accounts do not have access to the VMO2's workloads running within the virtualised environment.

3.5.6 The Supplier shall ensure that network oversight functions do not share trust domains or host pools with workloads that are not network oversight functions.

3.5.7 The Supplier will not deploy a network oversight function where the security of the envionment cannot be guranteed (e..g within a shared data centre).

3.5.8 The Supplier shall ensure that alarms shall be raised if logs stop being received from any network equipment

3.5.9 The Supplier shall treat their virtualisation infrastructure as a management plane, resulting in restriction of unnecessary access and appropriate segregation

Effective from 31st March 2028

3.5.10 The Supplier confirms that any network oversight function is operated within the UK and by UK-based employees.

3.5.11 The Supplier shall ensure where their virtualisation infrastructure allows virtual functions to have direct access to the physical hardware (cut-throughs), it is not be treated as a security boundary.

3.5.12 The Supplier shall ensure their virtualisation infrastructure is built and updated through an automated and verifiable process.

3.5.13 The Supplier shall use, wherever possible, automated and verifiable methods of configuration to adminster their virtualisation infrastructure.

3.5.14 The Supplier shall ensure that manual administration on their virtualisation infrastructure produces a real time alert and as a result notifies VMO2.

3.6 Controls applicable to vendors who provide deliver & configure services

Effective from 31st March 2024

3.6.1 Where the Supplier configures network equipment, (incl. both hardware & software) on the VMO2 network, they shall do so via secure, encrypted & authenticated means and ensure to disable all unnecessary network functions and/or equipment as a result.

3.6.2 The Supplier agrees to not use default passwords shall on any network equipment that is used within the VMO2 network or as part of a service that supports the VMO2 network.

Effective from 31st March 2025

3.6.3 Where the Supplier configures network equipment, (incl. both hardware & software) on the VMO2 network, they shall disable any default accounts associated with equipment or service in question.

Effective from 31st March 2027

3.6.4 The Supplier shall carry out administrative functions for new equipment via secure, authenticated & encrypted protocols as defined by VMO2.

3.6.5 The Supplier shall ensure each network equipment has strong unique credentials for every account.

3.7 Controls applicable to vendors who provide externally hosted infrastructure

Effective from 31st March 2027

3.7.1 Where the Supplier provides physical virtualisation infrastrcuture (combination of many hypervisors/physical servers/physical networking) to host network oversight functions, these shall:

- o - be robustly locked-down, use the latest patch for the software version and be in support.
- o not negatively impact the VMO2 network when updated;
- o restrict all incoming, apart from for management purposes, and outgoing connections;
- o only use known physical hosts;
- o use separate physical ports to segregate internal & external interface traffic;
- o limit the exposure of virtual workloads (e.g. disbaling virtual span ports by default);
- o be configured to prevent use of hard-coded MAC addresses, and
- o shall use encrpytion in transit and at rest where the security of transmission and/or the environment cannot be guranteed.

3.7.2 The Supplier will ensure all physical hosts are placed into a dedicated security pool, defined by the characteristics of those hosts (i.e. purpose, type of host etc..)

3.7.3 The Supplier shall ensure virtual workloads shall be tagged within a specific signed trust domain and be based on the risks associated with the workload.

3.7.4 The Supplier shall ensure that trust domains:

- o are separated from other trust domains;
- o are tagged by host pools that can execute them, and
- o use type-1 hypervisors to seperate domains and not containers, which can only be used to support a single trust domain

3.7.5 The Supplier shall ensure that physical host are not able to impact hosts in other host pools. (e.g. spoofing VLAN/VXLANs of virtual networks).

3.7.6 The Supplier shall ensure that any control and orchestration functions of their virtualisation infrastructure shall reside in a trusted physical and logical location.

3.7.7 The Supplier shall not run functions that support the adminstration and security of virtualisation infrastructure on the same infrastructure it is adminstering, instead will be treated as network oversight functions themselves, residing in a trusted physcial

and logical location.

3.7.8 The Supplier shall not use containers to separate network oversight functions from other network oversight functions and other functions.

Effective from 31st March 2028

3.7.9 The Supplier shall ensure that only physical hosts that are cryptographically attested to be in a known-good state can be provisioned into the virtualisation fabric.