Telefonica UK Security Schedule

Contents

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 Telefonica to ensure the integrity, security, resilience and confidentiality of Telefonica information and the Telefonica network.

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

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 Telefonica UK.

"**Data Protection Legislation**" means (a) 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. (b) all retained EU law as defined in the European Union (Withdrawal) Act 2018 and any other future EU law relating to personal data that becomes applicable in the UK as amended from time to time to the extent applicable to the processing activities or obligations under or pursuant to this Agreement. 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 provided by the Supplier pursuant to the Agreement.

"**Telefonica UK Information**" means all and any personal data as defined in the Data Protection Legislation. It also includes customer, employee data, confidential information, payment card data and/or other information or data processed, stored or accessed by Supplier on behalf of Telefonica in connection with the Agreement.

All references to the 'security' of **Telefonica UK 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.

1.0 Information Security

1.1 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 Telefonica UK and how these Services are used. This document must be made available to Telefonica UK within 30 calendar days of written notice.

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

1.4 Further, the Supplier must inform Telefonica UK (via the Business Owner) prior to any changes to the Services to Telefonica UK, 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 Telefonica UK 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 data breaches to Telefonica UK Information.

1.8 The Supplier must not implement any process or service which may put any Telefonica UK 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 Telefonica UK 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 Telefonica UK.

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 Telefonica UK.

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

1.16 The Supplier shall secure its networks and access connections in accordance with industry best practice to maintain appropriate protection of Telefonica UK Information.

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

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 perform regular vulnerability scans (at least annually) on any of the Supplier's IP addresses (internal or external) that create, store, transport, process, or delete Telefonica UK Information.

2.4 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 Telefonica UK information or support the Services.

3.0 Legal & Regulatory Compliance

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

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 Telefonica UK) must be validly owned or licensed by Supplier for the duration of the Agreement.

3.4 The Supplier shall procure that all employees, contractors and third party users involved in the provision of the Services enter into employment contracts which state their and Supplier's responsibilities for information security and confidentiality obligations with respect to Telefonica UK Information.

3.5 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.

3.6 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 as defined within the Data Protection Legislation. Data breaches shall be notified in accordance with paragraph 5.2 below.

3.7 The Supplier shall ensure that any service used to process and store Telefonica UK 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 service a subject access request, which has been made in accordance with the Data Protection Legislation.

3.8 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 Telefonica UK Information cannot be compromised.

4.2 Telefonica UK 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 Telefonica UK, the Supplier must respond to any requests for information or data to be provided to Telefonica UK in relation to the Services and Supplier's compliance with this Schedule within 30 calendar 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 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 Telefonica UK in writing of becoming aware of any Telefonica UK information data

breach. Data breach in this paragraph shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Telefonica UK 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 Telefonica UK 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 Telefonica UK by emailing security.incident@virginmediao2.co.uk

5.5 The Supplier shall provide, without delay, reasonable cooperation and assistance to Telefonica UK in the event of any data breach with respect to the Telefonica UK 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 Telefonica UK may have in the Agreement or at law, Telefonica UK 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. Telefonica UK shall not be liable to pay for any services(s) which are restricted or withdrawn pursuant to this paragraph.

6.0 Retention of Telefonica UK Information

6.1 The Supplier shall treat all Telefonica UK information provided to them as restricted and confidential, unless otherwise marked. The Supplier shall comply with all obligations relating to confidential information set out in the Agreement.

6.2 The Supplier shall comply with Telefonica UK's data retention policy (as amended from time to time). A copy of the policy is available at https://www.telefonica.com/en/about-us/suppliers/contracting-policies-and-conditions/.

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

6.4 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 Telefonica UK, the Supplier shall return all Telefonica UK Information and copies thereof to Telefonica UK, or shall destroy all this Information within 30 calendar days and certify to Telefonica UK that it has done so, unless legislation imposed upon the Supplier prevents the returning or destroying of all or part of the Telefonica UK Information transferred. In that case the Supplier warrants that it shall notify Telefonica UK 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 Telefonica UK Information. This includes:

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

6.4.2 any Telefonica UK Information retained by the Supplier's sub-contractors or any third parties used by the Supplier in the provision of the Services.

6.5 Where there is a need to dispose of media that contains or stores Telefonica UK 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.

6.6 All items of equipment containing Telefonica UK 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 Telefonica UK 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 Telefonica UK 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 Telefonica UK 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 Telefonica UK 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 Telefonica UK systems Supplier shall ensure that its personnel are uniquely authenticated using only user identifications provided by Telefonica UK, and that no system will be shared after user authentication.

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 Telefonica UK 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 Telefonica UK using the email address businesscontinuity@o2.com within 14 working 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 Telefonica UK, 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 Telefonica UK 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 Telefonica UK 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 Telefonica UK 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 Telefonica UK 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 Telefonica UK 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 checks on the right to work, employment references, 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 Telefonica UK 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 Telefonica UK's discretion.

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

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

legislation.

11.0 Audit

11.1 The Supplier shall permit Telefonica UK, or an independent representative, to perform an audit by providing no less than 30 days' notice. The Supplier will allow Telefonica UK 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. Telefonica UK shall not conduct an audit more frequently than once in any 12 month period, except in the event Telefonica UK 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 Telefonica UK's right to audit.

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

11.4 Telefonica UK 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 Telefonica UK 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 Telefonica UK 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 Telefonica UK Information shall have the entire device encrypted to a minimum symmetrical standard of AES 256-bit encryption (e.g. laptops, 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 Telefonica UK Fraud & 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 Telefonica UK by emailing security.incident@o2.com.

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 Vulnerability Management

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

13.2 Vulnerability response – 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)

13.3 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

13.4 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. 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 Telefonica's request.

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

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

13.7 The Supplier shall ensure any software developed by Supplier is tested every six months for security flaws and to create workarounds or patches to mitigate the vulnerability according to the requirements in 13.2.

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

13.9 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 Telefonica upon written request.

13.10 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.

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

13.12 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 Telefonica UK with evidence to show that support is available for this third party software for the lifetime of the Service.

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

14.0 Logging

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

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

14.3 Supplier shall protect and regularly review system administrator and system operator activities of systems that have access to Telefonica UK Information.

14.4 Supplier shall facilitate the complete and secure maintenance and retention of activity log record. Logs shall be retained for 12 months.

14.5 Supplier shall support Telefonica UK with the analysis and understanding of log information.

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

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 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. Telefonica UK 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 Telefonica UK 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 Telefonica UK from and against all penalties, costs and expenses which may be suffered, paid, or incurred by Telefonica UK 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 Telefonica UK's data retention policy.

1.5 The Supplier shall perform an annual PCI compliance assessment for all work relating to Telefonica UK 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 Telefonica UK.

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 Telefonica UK to include in its annual report (and/or the annual reports of other companies in the Telefonica UK 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 Telefonica UK'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 Telefonica UK'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 Telefonica UK, work with Telefonica UK 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 Telefonica UK 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 TELEFONICA UK, the Supplier must do an appropriate resilience risk assessment and disclose it to TELEFONICA UK.

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

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

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

5.5 Suppliers shall immediately (but no later than 48 hours) report and escalate all security incidents, vulnerabilities and misuse that could cause security risks to Telefonica UK in accordance with the Telefonica UK 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 TELEFONICA UK 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 TELEFONICA UK 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 TELEFONICA UK.

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.

Telefonica UK TSA Supplier Security Appendix

Contents

1.0 Purpose

This TSA Supplier Security appendix identifies additional security requirements for suppliers whose products or services are used by TELEFONICA UK in the delivery of its public electronic communications network or services.

If a Supplier has been identified as in scope for the Telecommunications (Security) Act 2021 (the "**TSA**") then they 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 TELEFONICA UK 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.

2.0 Controls applicable to all TSA vendors

Effective from 31st March 2024

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 Secuity Schedule) for TELEFONICA UK.

2.2 The Supplier will complete a TELEFONICA UK Shared Responsibility Matrix to be supplied by TELEFONICA UK detailing the responsibilities between TELEFONICA UK, 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 Telefonica 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 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, Telefonica UK 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 Telefonica UK in relation to the security of the Telefonica network, including those necessary to evaluate the security requirements of this TSA Supplier Security Schedule.

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

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

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

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

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

2.12 The Supplier shall ensure that any administrator controls they apply are at least as rigorous as TELEFONICA UK controls when the administrator has access to the provider's network or service or to sensitive data.

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

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

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 with third party administrative access (3PA)

Effective from 31st March 2024

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

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 TELEFONICA UK.

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 TELEFONICA UK's network.

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

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

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

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

Effective from 31st March 2024

3.2.1 The Supplier must provide to TELEFONICA UK 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 (Network Equipment Security Questions)

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

3.2.3 Should the Supplier provide hardware or software to TELEFONICA UK, they confirm they will respond to TELEFONICA UK's request to complete Annex B of the TSA (Network Equipment Security Questions) allowing TELEFONICA UK to understand the practices in place to develop hardware and software.

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

3.2.5 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.

3.2.6 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.

3.2.7 The Supplier shall remediate any security issue that poses a security risk on the TELEFONICA UK 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.

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

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

3.2.10 The Supplier shall provide reasonable support to review, manage, and/or replace any unsupported equipment supplied by it, as required by TELEFONICA UK.

Effective from 31st March 2025

3.2.11 Where the Supplier uses third-party testing, the Supplier shall ensure this is repeatable, performed independently of the Supplier and is clearly applicable to TELEFONICA UK's deployment.

3.2.12 All equipment should be updated within 90 days of the release of any relevant and appropriate version; however, critical security patches shall be prioritised over functionality upgrades.

3.3 Controls applicable to SIM manufacturers

Effective from 31st March 2024

3.3.1 Where the Supplier provides a product or service relating to UICC/SIM cards, they shall ensure the protection of information and configuration, such as keys, algorithms, and applets, associated with such equipment annually.

Effective from 31st March 2025

3.3.2 Where the Supplier provides fixed-profile SIM cards to TELEFONICA UK, the Supplier shall ensure that sensitive SIM data is appropriately protected, and the confidentiality, integrity and availability of such data shared is protected at every stage of the SIM lifecycle. Access to such data should be strictly limited to appropriate employees.

3.3.3 Where the Supplier provides fixed-profile SIM cards to TELEFONICA UK, on request from TELEFONICA UK, the Supplier shall demonstrate that SIM cards are independently audited. E.g., Through GSMAs SAS Scheme.

3.4 Controls applicable to vendors who provide customer premise equipment

Effective from 31st March 2024

3.4.1 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.

Effective from 31st March 2025

3.4.2 The Supplier shall have a documented roadmap of future software implementation showing versions and “end of life” or “end of support” detail to avoid the solution retaining out of date software for any longer than necessary. Replacements should be offered as soon as reasonably practicable after CPE is out of support. This includes any third-party software included in the solution.

3.4.3 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).

3.4.4 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 a network oversight function

Effective from 31st March 2027

3.5.1 The Supplier must appropriately design and segregate network oversight functions (NOFs) securely from other parts of TELEFONICA UK's or Supplier's network, with NOFs being housed and operated on trusted platforms. Network oversight functions 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 security compromise which the patch or mitigation addresses.

3.5.2 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 must ensure that all user access on network oversight functions is limited to a minimal set of trusted privileged users based on least privilege, pre-authorised by TELEFONICA UK and identifies a user individually.

3.5.5 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.

3.5.6 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.

Effective from 31st March 2028

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