Schedule (insert number)

Security

1.0 Information Security

1.1 For the purposes of this Schedule "**Telefónica Information**" means all and any Personal Information as defined in GDPR, Customer Data, Confidential Information, PCI Data and/or other information or data processed by Supplier (or any of its sub-contractors) on behalf of Telefónica in connection with the Agreement.

1.2 The Supplier shall comply with Telefónica Security Policy.

1.3 The Supplier shall advise Telefónica or their agents on request, of any areas of non-compliance with Telefónica Security Policy.

1.4 All references to the 'security' of **Telefónica Information** shall take into account the protection of the confidentiality, integrity and continued availability of this information as applicable to the services being provided.

1.5 The Supplier shall design, implement and maintain a documented Information Security Management System sufficient for and enabling Telefónica to be certified to ISO/IEC 27001:2013 information security management systems. Copies of these plans are to be made available to Telefónica plus evidence provided on request demonstrating management and review of these plans.

1.6 The Supplier shall design and implement processes that minimise the risk to **Telefónica Information** and such processes must be aligned to Telefónica stated requirements.

1.7 Where the Supplier's service to Telefónica requires the processing of Telefónica Customer Information or Data, this must be undertaken in accordance with Telefónica stated requirements and/or as an authenticated and authorised request from the named Telefónica Customer.

1.8 The Supplier must not implement any process or service which may put any Telefónica network, system or on-line services at risk; for example by issuing a high frequency of requests that could adversely affect the service for others.

1.9 The Supplier shall maintain an up to date document detailing what services they provide for Telefónica and how these services are used. This document must be made available to Telefónica within 30 days of notice. Furthermore, the Supplier must inform Telefónica (via the Account Manager) prior to any changes to the way **Telefónica Information** services are to be used. Such notification should include an impact assessment relevant to the proposed changes.

1.10 The Supplier shall treat all **Telefónica information** provided to them or provided by Telefónica agents on its behalf as confidential (i.e. 'In Confidence' as defined in Telefónica Security Policy) unless otherwise marked and ensure policy compliance is achieved when processing, transmitting or storing such information. This equally applies to their nominated agents or contractors.

1.11 The Supplier shall establish processes to keep up to date with emerging security threats and vulnerabilities and ensure that the relevant security controls are implemented to maintain compliance with Telefónica Security Policy.

1.12 Appropriate measures shall be implemented to prevent and/or detect potential fraud, such measures not being greater or more onerous than those followed by Telefónica.

1.13 The Supplier shall perform regular vulnerability scans (at least annually) on any of the Suppliers IP addresses (internal / external) that retain, transmit, or process **Telefónica Information** at Supplier's cost.

1.14 The Supplier shall arrange for independent annual security penetration testing of their services at the Supplier cost. All results that impact the Telefónica Agreement shall be shared with Telefónica. Any service that is associated to a compliance or standard, must be delivered to meet that compliance or standard

1.15 Telefónica reserve the right to approve the Supplier's used in clause 1.13 and 1.14 above.

1.16 A system security patch management regime, with regular updates, must be implemented to ensure ongoing system integrity when new security vulnerabilities are discovered. Applicable systems shall include those which are used to store, process or otherwise protect **Telefónica Information**.

1.17 System security configuration must be implemented in accordance with industry best practice security standards. It is Telefónica's recommendation that the Centre for Internet Security benchmarks (http://benchmarks.cisecurity.org/) is used.

1.18 Web applications must be tested against OWASP criteria (https://www.owasp.org/) to ensure that they are not vulnerable to the OWASP top ten risks as a minimum requirement.

1.19 Where relevant, adequate controls shall be put in place to ensure that user and/or customer actions and events are legally binding and cannot be repudiated and that such actions are accountable to an identifiable individual.

1.20 The Supplier shall maintain a list of any devices or media used by the Supplier, but owned by Telefónica and adhere to Telefónica instructions to either return to Telefónica or destroy such devices or media if requested and authorised.

1.21 The Supplier shall ensure that all accesses to **Telefónica Information** shall be accountable to an identified person or machine process.

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

1.23 Where there is a need to dispose of media that contains or stores **Telefónica 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.

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

1.25 The Supplier shall ensure appropriate detection, prevention and recovery controls to protect against malicious code (e.g. viruses) in all systems used to store or process Telefonica information or support the service provided to Telefonica.

1.26 The Supplier shall allocate security roles and responsibilities for contracted employees.

1.27 The Supplier shall maintain a documented security escalation process, which includes the requirement to notify Telefónica upon any actual or suspect security breach may impact any aspect of the processing or storage of **Telefónica Information** or systems that support the service provided to Telefonica.

1.28 The Supplier shall secure its networks to maintain appropriate protection of **Telefónica Information**. All access connections shall be secured using TLSv1.2 unless otherwise agreed.

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

1.30 The supplier shall ensure that any service used to process and store **Telefónica Information** has the capability to extract and export such data quickly, normally within 5 working days, in order to service a Subject Access Request, which has been made in accordance with the Data Protection Legislation.

2.0 Portable Device Security:

2.1 Any portable device that is used to store or accesses **Telefónica Information** shall have the entire device encrypted to a standard equivalent to FIPS 140 – 2 and FIPS -197 (e.g. laptops, USB flash drives, memory sticks, and other removable media).

2.2 The device security shall ensure that:

2.2.1 Temporary storage areas are encrypted;

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

2.2.3 The entire device shall automatically encrypt after 15 minutes inactivity;

2.2.4 Users are able to lock the device manually before periods of inactivity;

2.2.5 The passphrase used shall adhere to Telefónica's password policy.

2.3 Where the entire device cannot be encrypted, all data contained within the device shall be encrypted to a standard approved by the Telefónica Fraud & Security Team.

3.0 Security Standards

3.1 Where the Supplier is processing or storing Telefónica Customer Data, on a regular basis, there will be a requirement for the Supplier to be:

3.1.1 independently certified to ISO/IEC 27001:2013 in their own right, with a scope which covers Telefónica Customer Data;

3.1.2 Independently tested to verify that the systems used to process Telefónica Customer Data meet

the requirements of the UK Government promoted Cyber Essentials scheme.

4.0 PCI DSS (Payment Card Industry Data Security standard)

4.1 Where the Supplier is transmitting, storing and or processing Payment Card Data, 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. Telefónica 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 Telefónica any identified vulnerability per PCI DSS requirements.

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

4.3 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 Telefónica's information retention policy as issued from time to time.

4.4 The Supplier shall perform a PCI compliance assessment for all work relating to Telefónica and perform any remedial action required within a timescale agreed with Telefónica.

5.0 Information / Data Retention

5.1 The Supplier shall comply with Telefónica's data retention policy (as amended from time to time). A copy of the policy can be supplied by Telefónica together with any subsequent amendments upon request. Any changes to the data retention policy resulting in a material increase in costs shall be dealt with by the change procedure.

5.2 The parties agree, that at the request and choice of Telefónica, the Supplier shall return all **Telefónica Information** and copies thereof, to Telefónica, or shall destroy all this Information within 30 days and certify to Telefónica that it has done so, unless legislation imposed upon the Supplier prevents the returning or destroying of all or part of the **Telefónica Information** transferred. In that case the Supplier warrants that it shall notify Telefónica of the Information being retained and the Supplier shall guarantee the confidentiality of the Information and shall not actively process the Information anymore. This includes:

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

5.2.2 Any material (information/data) retained by the Supplier's sub-contractors.

5.2.3 Requirements on termination of the provision of Services

6.0 Sarbanes Oxley Compliance:

6.1 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 Telefónica to include in its annual report (and/or the annual reports of other companies in the Telefónica Group on form 20-F ("Annual Report") a report of management on internal controls over financial reporting.

6.2 It is further understood by the parties that the Telefónica's auditor (and/or the auditors of other companies in the Telefónica 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").

6.3 Where relevant to the contracted services, the Supplier may be required to provide information applicable to Telefónica's compliance requirements to clauses 6.1 and 6.2 above.

7.0 CAS(T) (Applicable to communication services or other elements linked to the TUK CAS(T) scope)

7.1 The Supplier acknowledges and agrees that the Services will need to be compliant to government guidelines regarding the CAS(T) Information Security Standard. Accordingly, once such requirements have been agreed between the parties, the Supplier shall be compliant to the following information assurance requirements to the same degree as the Customer and, if appropriate, hold the necessary certifications in respect of the following:

7.1.1 the applicable security requirements as specified under HMG Security Procedures - Telecommunications Systems & Services (current version is August 2016 Issue 3.0), which shall be audited under the NCSC scheme known as CAS(T) to meet the baseline conditions;

7.1.2 compliance with the requirements of Data Protection Legislation (within the EU this will equate to GDPR), Freedom of Information Act 2000 and related legislation and guidance/codes of practice where necessary;

7.1.3 make the necessary changes/adjustments requested in writing by the Customer from time to time to deal with changing legal or industry standards, or changes to any Customer Policy relevant to CAS(T) or any replacement standard/requirement equivalent; and

7.1.4 any other specific requirements notified to the Supplier by the Customer which are required to be flowed down to the Supplier as a result of any contract under negotiation or entered into in respect of CAS(T) services to be provided by the Customer.

8.0 Access Control

8.1 The Supplier shall ensure that there is no sharing of account ID's and passwords or actual accounts.

8.2 System access to **Telefónica Information** shall include an automatic password protected inactivity time- out function that shall operate when the keyboard has not been used for in excess of 15 minutes.

8.3 All users shall follow good security practices in the selection and use of passwords, as detailed in Telefónica Security Policy.

9.0 Business Continuity

9.1 The Supplier shall provide a copy of their Business Continuity Policy and a Business Continuity Plan that demonstrates how they will maintain the contracted service level in the event of an emergency. Business Continuity Policy and Planning must align with the best practice detailed in the standard ISO 22301 Business Continuity Management.

10.0 Legal & Regulatory Compliance & Telefónica Requirements

10.1 The Supplier shall comply with Telefónica's requirements and direction on security.

10.2 The Supplier shall segregate **Telefónica Information** (servers/applications/physical environment) from the Suppliers other client's data or agree with Telefónica, compensating controls to provide such segregation.

10.3 The Supplier shall comply with all legislation, regulations and codes of practice provided by Telefónica, including, but not limited to the Data Protection Legislation.

10.3.1 With regards to the Data Protection Legislation, it will be agreed as part of contract where ownership of data lies and the responsibilities of Data Controller and Data Processor as defined within the Act

10.4 The Supplier shall comply with all Telefónica's supplier policies published on http://www.telefonica.com/en/about_telefonica/html/suppliers/modelo_compras/supplier_policies.shtml, which are a subset of Telefónica Security Policy.

10.5 The Supplier agrees and warrants:

10.5.1 That it has no reason to believe that any legislation applicable to it prevents fulfilling compliance with this clause;

10.5.2 To notify Telefónica of any legally binding request for disclosure of personal data by a law enforcement authority.

11.0 Breaches, Compliance Failures and Fraud & Security Issues

11.1 The Supplier shall have a process in place which ensures that they identify and address potential breaches and compliance failures.

11.2 The Supplier shall co-operate with Telefónica on fraud and security issues relating to any of their employees as far as they are able to, having regard to all applicable regulation and legislation.

11.3 The Supplier shall inform Telefónica within a reasonable time-period (normally 1 working day) in the event of any breach of security, which may affect **Telefónica Information** or the services related to the processing of this Information.

11.4 The Supplier shall notify the Telefónica Account Manager if **Telefónica Information** is received from Telefónica, or is being sent to Telefónica, that does not comply with Telefónica Security Policy. This includes Information sent or received from Telefónica agents.

11.5 The Supplier shall undertake to reimburse Telefónica for any financial losses resulting from fraudulent or negligent activity by their employees.

11.6 Telefónica reserves the right to restrict or withdrawn service where the service is either being misused (i.e. not used in according with Telefónica requirements) or the continuity of the service is put at risk.

12.0 Building Design:

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

12.2 Suitable access points (if not via the main entrance) shall be provided for disabled and goods delivery access.

12.3 Access to the areas used to process or store **Telefónica Information** shall be physically controlled (e.g. electronic access control system.)

12.4 Access to the areas processing or storing **Telefónica Information** should be restricted to those people working on the Telefónica contract or those who have an operational requirement to access the area.

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

12.6 All final fire exit doors shall be fitted with suitable escape mechanisms (e.g. 3 point hardware). Other doors which form part of the external building shell shall be locked secure when not in use.

12.7 Computer room walls shall be block-work wall construction or have enhanced security partitioning built slab to slab. Computer rooms shall not form part of external elevations. Where building design dictates this is not possible and the external elevation includes windows, an assessment of the external glazing is required and if deemed applicable additional protection shall be be required I.e. security bars, window film or secondary glazing. Additional electronic monitoring shall be deployed to where the computer room has an external elevation e.g. vibration and, or acoustic break glass detection.

12.8 An electronic access control system shall be installed to control and manage access into the building and internal areas used to process and store Telefónica Information. The system should log all activities, alarms and events and hold data for a minimum of 90 days.

12.9 There shall a defined and documented procedures in place to manage visitor and temporary access into the building and internal areas used to process and manage Telefónica Information.

12.10 A BS EN 50131-1 Grade 2 or Grade 3 intruder detection system shall be installed. The system shall be monitored locally at a security monitoring station and have the capability to be remotely monitored by an external alarm receiving centre. .

12.11 A CCTV system shall be used to monitor the external building elevations, the main reception area, any other staff entrance points, the goods delivery point(s), the external fire exit doors from the building and the entry / exit point into the area(s) processing the **Telefónica Information** The system shall maintain a minimum of 30 days recording.

12.12 External lighting for the building shall support any external elements of the CCTV system and give sufficient lighting for natural observation. Where this is not possible the CCTV system shall include infra-red lighting.

12.13 All electronic security systems (Electronic Access Control, IDS and CCTV) shall have a maintenance programme in place, to ensure the systems are correctly calibrated, tested and functionality properly.

12.14 Appropriate protection and operational controls shall be provided for critical plant areas that support the building operation access.

13.0 Staff Criminal Records Checks

13.1 The Supplier shall carry out background verification checks on all existing and new employees including contractors, sub-contractors, agency workers, third party users (and any like persons) in accordance with relevant laws and regulations who are employed on the Telefónica contract prior to them having access to Telefónica Information.

13.2 The Supplier shall

13.2.1 Make sure that such a person is bound by an appropriate confidentiality agreement;

13.2.2 Perform a thorough background check on such person, including right to work, employment references, relevant qualifications and ensure that such person has no unspent criminal convictions which would question their honestly, integrity and suitability to be employed on this Telefónica contract;

13.2.3 sure that such person has an appropriate and valid security clearance where appropriate.

13.3 The Supplier shall comply with all reasonable requests in respect of the deployment of individual employees engaged on the Telefónica contract. The Supplier shall not be required to act in a discriminatory or unlawful way, but shall be expected to comply with requests for the non-recruitment or the removal of individuals from the Telefónica contract at Telefónica's discretion

14.0 Right to Audit

14.1 The Supplier shall permit Telefónica or its agent or representative at all reasonable times and on reasonable notice to enter any place used by the Supplier in connection with the provision of the Services for the purpose of inspecting and verifying the compliance of the Supplier with its obligations under this Schedule. Furthermore, documentation, computers, word processors or other similar machines in its possession, custody or control for such purpose. Nothing in this paragraph shall oblige the Supplier to disclose details of other customers of the Supplier and/or information which is confidential to the Supplier.

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

14.3 The Supplier shall permit Telefónica or its agent or representative at all reasonable times and on reasonable notice to undertake security penetration testing and/or vulnerability testing on any service which is used to process Telefónica or its customer's data.

15.0 Compliance

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

15.2 Telefónica 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 above.

15.3 Unless otherwise stated, The Supplier must respond to any requests for information or data to be provided to Telefónica in relation to the Supplier services within 30 days of notice.

16.0 Exit Audit

16.1 Where the contract between Telefónica and the Supplier has ended, the Supplier shall submit its data processing facilities and that of its sub-processing facilities (e.g. suppliers, sub-contractors, operating companies) for an audit by Telefónica or their appointed 3rd Party (known as the Exit Audit).

16.2 The Supplier shall confirm if they are retaining any Telefónica material (e.g. for legal reasons), this shall be declared to Telefónica prior to the termination of the service and the reason for retention provided (electronic and/or hard-copy). This shall include any material retained by the Supplier's sub-contractors.

17.0 Patching

17.1 Supplier shall, without delay, assist and co-operate with Telefónica in implementing the measures required to correct any non-compliance with Suppliers security obligations, as detected in audits or otherwise detected by either party**.**

17.2 Supplier shall immediately (but by no later than 24 hours) report and escalate all security incidents, vulnerabilities and misuse that could cause security risks to Telefónica in accordance with the Telefónica corporate information security policy and all technical or administrative security rules or procedures that arise from it.

17.3 Security patches – critical and non-critical- shall be treated as requests that will include a required period of time for their installation. UK security patches shall be implemented within 30 calendar days, unless otherwise agreed, and critical patches shall be installed within 5 calendar days. Supplier must maintain documentary evidence on patching installations details and supply such evidence on Telefónica's request.

17.4 Supplier shall analyse potential effects on existing systems of security patch application, coordinating this activity with other service management groups.

17.5 Supplier shall participate in meetings and committees relating to the security process as requested by Telefónica.

17.6 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.

17.7 Supplier shall train, inform and educate its employees and contractors about **Telefónica information** security policies and best practice in relation to information security, and provide evidence thereof to Telefónica upon request.

17.8 Supplier shall immediately (but by no later than 24 hours) inform Telefónica in writing, within 24 hours, of becoming aware of any data breach or incident of non-compliance of its security obligations.

17.9 Supplier shall ensure any software created by themselves is developed using OWASP secure coding guidelines and tested every six months for security flaws and to create workarounds or patches within 30 working days to mitigate the flaw.

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

17.11 The supplier shall provide a list detailing all software applications that are required as part of the solution for support purposes.

17.12 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 solution.

17.13 The supplier shall document any third party software included in the solution and shall supply Telefonica with evidence to show that support is available for this third party software for the lifetime of the overall system.

18.0 Logging

18.1 Supplier shall support the population of the central audit mechanism. The central audit mechanism is a tool that collects and stores the required security logs as defined by the Telefónica security policy.

18.2 Supplier shall support security log consolidation while still allowing the processing, and analysis required to extract the required security data.

18.3 Supplier shall facilitate the complete and secure maintenance and retention of activity log record and records.

18.4 Supplier shall support the analysis and understanding of log information.

18.5 Supplier shall guarantee that its personnel will be uniquely authenticated when logging into Telefónica systems using only user identifications provided by Telefónica, and that no system will be shared after user authentication.

19.0 NIS Directive

19.1 The Supplier acknowledges and agrees that the Services will need to be compliant to government guidelines regarding the NIS Directive.

19.2 The Supplier agrees to assist Telefonica to ensure compliance.

19.3 The Supplier will provide monthly Key Performance Indicators ("KPIs") evidencing compliance with the requirements set out in this Security schedule and any other KPIs as agreed between the parties from time to time.

Note.

- Security data / information will include: vStart date and time, end date and time, usage/actioned performed, IP address, username – refer to logging policy on intranet, vRetention period to be 90 days minimum, rolling buffer (circular = losing 1st day)

1.1 The supplier is responsible for the security of the services provided to Telefónica Supplier's cost

1.2 The supplier must ensure that security forms part of their product lifecycle and roadmap

DOCUMENT INFORMATION

Document name:	Security Schedule
Brief description:	Security requirements for suppliers
Document Owner:	Nigel Watson and Sean Portsmouth
Date of Issue:	March 2014
Next review date:	August 2019

CHANGE HISTORY

Version No.	Issue Date	Changed by	Changes
1.0	March 2014	Sean Portsmouth	Document created
1.1	March 2014	Sean Portsmouth	Revised and updated
1.2	March 2014	Sean Portsmouth	Revised, updated and circulated
1.3	May2015	Sean Portsmouth	Amends made to section 11.1
1.4	July 2015	Nigel Watson	Various updates and new additions, including updates to 27001 compliance & Cyber Security Essentials requirements
1.5	April 2016	Sean Portsmouth	Added Section 17.0 and 18.0 Patching and Logging
1.6	August 2016	James Cheung	Changed 1.28 web access connections
1.7	January 2018	James Cheung	Changes to 1.13, 1.14, 4.1, 12.3, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13, 12.14
1.8	August 2018	James Cheung	GDPR, CAS(T), NIS Directive

CIRCULATION LIST

Fraud and Security	Fraud and Security	Procurement	Legal
Sean Portsmouth	Dean Di Pasquale	Keithley Martin	Megan Bawden
Caroline Maloney	James Cheung		