Contents

PART 1: INTRODUCTION

1.1 This document sets out BT's security requirements.

1.2 In these Security Requirements, the definitions in Part 5 headed "Definitions" will apply, but otherwise the terms of the Contract shall apply to these Security Requirements and all words and expressions used in these Security Requirements shall bear the same meaning given to them in the Contract.

1.3 These Security Requirements are in addition to and without prejudice to any other obligations of the Supplier in the Contract (including, without limitation its obligations under the Conditions headed "**Confidentiality**", "**Protection of Personal Data**" and "**Compliance**").

PART 2: LIMITED ACCESS REQUIREMENTS

This section will be advised as applicable where the Supplier will be providing Supplies that involve limited access to BT or BT Customer Information, or have user level access to BT's Administrative Systems. Suppliers who fall into this category will not be required to comply with any other parts of this document.

2. Without prejudice to any obligations of confidentiality it may have, where the Supplier or Contract Personnel have access to BT Information, the Supplier shall:

2.1. Ensure BT Information is not disclosed to or accessed by Contract Personnel unless necessary for the provision of the Supplies; and

2.2. Put in place all systems and processes (both technical and organisational) as are required in accordance with Good Industry Security Practice to protect the security and confidential of BT Information and BT Systems.

PART 3: GENERAL SECURITY REQUIREMENTS

Mandatory where Part 2: Limited Access Requirements has not been advised as applicable.

3. GENERAL INFORMATION SECURITY

General Information Security

3.1. The Supplier shall implement systems and processes (both technical and organisational) to:

3.1.1. protect the security and confidentiality of BT Information and BT Systems as mandated by in these Security Requirements; and

3.1.2. ensure the availability, quality, integrity and adequate capacity to deliver the Supplies without interruption, as required by Good Industry Security Practice.

3.2. The Supplier shall implement a documented IT change management process to ensure any changes to processes and Supplier Systems are implemented in a way that maintains the Supplier's compliance with these Security Requirements.

3.3. The Supplier shall make available to BT on BT's written request copies of any security certifications and statement of compliance relevant to the Supplies in order to illustrate evidence of compliance with these Security Requirements.

3.4. The Supplier will take all reasonable steps to ensure appropriate individual(s) are appointed and made responsible as Point of Contact for Security Risk, Incident Management and Compliance Management. The Supplier shall notify BT Security Contact of the individual(s) Contact details and any change to them. Details should include:-

name, responsibility, role and group email address and/or telephone number

3.5. The Supplier acknowledges and agrees that from time to time BT may make reasonable changes to the BT Security Requirements where:

3.5.1 the Supplier is subject to a merger, acquisition, or material changes in ownership or control;

3.5.2 there is a change to technology or industry security standards; or

3.5.3 there are any material changes to the Supplies or how they are provided,

(each a "Security Requirement Change").

Upon the upon receipt of written notification from BT of the need for a Security Requirement Change, the Supplier shall comply with a Security Requirement Change promptly, and in any event within a reasonable time (such reasonable time to take into account the nature of change and the risk to BT).

3.6. The Supplier shall, as a minimum annually or when there are any material changes to the Supplies or how they are provided, review the Security Requirements to ensure they are still compliant to all applicable Security Requirements.

3.7. If the Supplier subcontracts obligations under the Contract, then the Supplier shall ensure all contracts with relevant Subcontractors, include written terms requiring the Subcontractor to comply with BT's Supplier Security Requirements to the extent they are applicable. These terms must be in place between Supplier and its Subcontractor before the Subcontractor or any of its personnel can access BT Systems and BT information.

Use of BT Information

3.8. The Supplier shall not use BT Information for any purpose other than for the purpose for which it was provided to the Supplier and then only to the extent necessary to enable the Supplier to perform the Contract. Where the Supplier is Processing Personal Data, it shall not use any Personal Data which forms part of the BT Information for any purpose other than for the purpose specified in the Processing Appendix.

3.9. BT Information may be retained for as long as necessary to perform the Contract, after which it should be retained no longer than a maximum of two years unless a different retention period has been agreed between BT and Supplier or is required by any applicable laws. For the avoidance of doubt where the Supplier is Processing Personal Data, it shall not retain any Personal Data which forms part of the BT Information for longer than the periods specified in the Processing Appendix or the Condition headed "Protection of Personal Data".

3.10. The Supplier must abide by applicable policies and standards at: http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm.

3.11. If the Supplies are in direct support of a UK Government contract, the Supplier must comply with the most current version of the Cyber Essentials Plus.

Information Handling

3.12. The Supplier shall have and follow information handling processes which are materially consistent with the Third Party Information Classification and Handling Specification and which as minimum shall ensure the Supplier:

3.12.1. implements appropriate processes to prevent the unauthorised distribution of BT Information in any form, including by email, fax, social media, print or post (for example ensuring that a clear desk and screen policy is in place and In Strictest Confidence Information is not sent by fax or email);

3.12.2. does not discus BT Information in meetings unless all attendees are: (i) authorised to attend the meeting; (ii) need to know the information being discussed; and (iii) are aware of, and consider, their confidentiality obligations;

3.12.3. does not store BT Information:

3.12.3.1. in the cloud or with internet services including, but not limited to, Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin or Facebook unless agreed in writing with BT;

3.12.3.2. on any laptop or other device unless it is protected with a full disk encryption feature (such as BitLocker) that meets the standards at paragraph 3.16; or

3.12.4. deletes or puts BT Information beyond use of daily business activities in a secure manner.

Access Control

3.13. The Supplier shall maintain access controls on Supplier Systems appropriate to the environment and nature of the Supplies supplied to BT including ensuring where applicable that:

3.13.1. all users, including administrator level users, shall have unique ID's;

3.13.2. regular password changes (at a minimum every 90 days) are required;

3.13.3. appropriate protections are implemented following unsuccessful login attempts to prevent brute force attacks;

3.13.4. unused accounts are automatically disabled;

3.13.5. passwords of an appropriate strength (with a minimum of 8 characters requirement incorporating three of the following categories: (i) upper case; (ii) lower case; (iii) numeric; and (iv) non-alpha numeric) are used and password history is enforced to prohibit the use of previous passwords within a 12 month period;

3.13.6. role-based access to Supplier Systems is implemented with as a minimum more stringent access controls for administrator access; and

3.13.7. regular reviews and audits of user access are undertaken.

Remote Access

3.14. The Supplier is not permitted to allow Contract Personnel to Remote Access information classified as In Strictest Confidence unless otherwise agreed with BT in writing. Where Remote Access is permitted, the Supplier shall ensure that Remote Access is subject to appropriate security controls within Supplier's organisation, including but not limited to ensuing Remote Access by users being subject to strong two factor authentication. If Remote Access via public networks for support purposes is utilised, the connections will be encrypted in accordance with the standards of set out in paragraph 3.16.

Transmission of Data

3.15. Transmission of routine Bulk Records of BT Information should be via PGP or an industry approved transfer platform.

Encryption

3.16. The Supplier shall ensure In Confidence and In Strictest Confidence BT Information is encrypted both at rest and in transit, in accordance with Good Industry Security Practice ensuring that standards deprecated by the relevant industry are not used. Current encryption standards approved by BT at the Commencement Date which meet the requirements of this paragraph 3.16 are set out in the Third Party Information Classification and Handling Specification.

Patching

3.17. The Supplier shall have and follow a documented patch management process which as a minimum shall ensure that the Supplier:

3.17.1. deploys patches within the following timeframes:

Patch Type	Description	Timeframe
Critical patches	Patches necessary to address zero day vulnerabilities	As soon as practicable and in any event within 14 days of a patch becoming available
Important patches	Vulnerabilities classified as High 7.0 - 8.9 on the qualitative severity rating scale from the Common Vulnerability Scoring System (CVSS)	Within 30 days of a patch becoming available
Other patches	All patches that aren't important or critical patches	Within 8 weeks of a patch becoming available

3.17.2. monitors all applicable vendors for patch releases;

3.17.3. uses patches obtained from: vendors directly for proprietary systems and patches that are either (i) digitally signed or (ii) verified via the use of a vendor hash (MD5 hashes must not be used) for the update package such that the patch can be identified as coming from a reputable support community for open source software;

3.17.4. tests all patches on systems that accurately represent the configuration of the target production systems before deployment of the patch to production systems and that the correct operation of the patched service is verified after any patching activity; and

3.17.5. maintains and updates Supplier Systems to ensure the most up to date vendor patches can be applied.

3.18. If a system cannot be patched by the Supplier, the Supplier must notify BT in writing. On receipt of such a notification, BT shall review the risk to BT and BT Information associated with the continued use by the Supplier of the system and BT may require the Supplier to undertake any reasonable steps (at the Supplier's cost) to address any such risks.

Vulnerability Management

3.19. The Supplier shall have and follow a vulnerability management process which as a minimum shall ensure that the Supplier:

3.19.1. takes appropriate actions (for example scanning) to identify vulnerabilities;

3.19.2. undertakes its own regular penetration testing; and maintains reports of such testing; and

3.19.3. reacts to any notification of vulnerabilities and implements action plans to mitigate known vulnerabilities in accordance with paragraph 3.26 to 3.31.

Pen Testing

3.20. The Supplier shall:

3.20.1. permit BT (or authorised BT subcontractors) to carry out reasonable penetration testing on reasonable notice; and

3.20.2. provide BT access to existing Supplier penetration test reports relevant to the Supplies being provided.

Audit and Logging

3.21. The Supplier shall have and shall follow an audit and logging process which as a minimum shall ensure that the Supplier logs (as appropriate) the following events:

3.21.1. the start and stop points of the logged process;

3.21.2. changes to the type of logged events as required by the audit trail (for example the start-up parameters and any changes to them);

3.21.3. Supplier System start-up and shut-down;

3.21.4. successful logins;

3.21.5. failed login attempts (for example wrong user ID or password);

3.21.6. all operations performed by privileged users (for example users with powerful access to system utilities or applications);

3.21.7. successful and unsuccessful privilege escalation;

3.21.8. all access by the Supplier or Supplier Contract Personnel to or operations on In Strictest Confidence Information; and

3.21.9. creation, modification and deletion to/of user accounts.

3.22. For each auditable event, the Supplier shall maintain a tamper proof audit trail that enable the reconstruction of such events.

3.23. Taking into account the criticality of the component/data, the Supplier shall regularly inspect and analyse audit logs to detect suspicious or anomalous behaviour and take appropriate action and/or raise an alarm.

3.24. All alarms must be documented and acted upon in a timely manner determined by the criticality of the alarm.

3.25. Supplier shall retain all log files for 3 months (unless other required to delete these pursuant to the Condition headed "**Protection of Personal Data**") and shall produce copies or permit access to the logs files at BT's request in a format agreed by both Parties**.**

Threat Management and Incident Handling

3.26. The Supplier shall have and shall follow a formal security incident management process which includes defined responsibilities for addressing a Relevant Security Incident. Any information related to a Relevant Security Incident shall be treated "**In Confidence**".

3.27. The Supplier shall inform the BT Security Contact and the BT Commercial Contact, within a reasonable period of time upon its becoming aware of any Relevant Security Incident, and in any event, no later than twelve (12) hours from the time the Relevant Security Incident comes to the Supplier's attention.

3.28. Without unreasonable delay, the Supplier shall promptly take appropriate and timely corrective action to mitigate any risks and effects related to the Relevant Security Incident in order to reduce the severity and duration of the incident.

3.29. The Supplier agrees to provide all information reasonably required by BT in respect of a Relevant Security Incident including but not limited to the:

3.29.1. date and time;

3.29.2. location;

3.29.3. type of incident;

3.29.4. impact;

3.29.5. classification of information impacted;

3.29.6. status; and

3.29.7. outcome (including the resolution recommendations or actions taken).

3.30. The Supplier shall ensure that identified risks as to the confidentiality, integrity or availability of BT Information in the Supplier's processes or Supplier Systems, are promptly remedied.

3.31. If a Relevant Security Incident is also a Personal Data Breach then the Supplier shall also adhere to the provisions of the Condition headed "**Protection of Personal Data**" in addition to the provisions of these Security Requirements. For the

avoidance of doubt the Supplier shall also adhere to the provisions of the Condition headed "**Protection of Personal Data**" in respect of all Personal Data Breaches notwithstanding the breach may, or may not be, a Relevant Security Incident.

4 CONTRACT PERSONNEL SECURITY

4.1 Contract Personnel shall not be granted Access until they have completed BT's Security of Information Training accessible via https://workingwithbt.extra.bt.com or via BT's learning system where the Contract Personnel have been allocated a BT identification number. BT's Security of Information Training must be refreshed from time to time, as detailed at https://workingwithbt.extra.bt.com. Supplier shall maintain the records of training and make these available for audit by BT.

4.2 Supplier shall ensure that all Contract Personnel sign confidentiality agreements that include materially similar obligations as those imposed on the Supplier in Part 2 above, before any Contract Personnel start working in BT buildings or on BT Systems or have access to BT Information. These confidentiality agreements must be retained by Supplier and be made available for audit by BT.

4.3 The Supplier shall deal with breaches of Supplier's and BT's security policies and procedures, through formal processes including disciplinary action which may include removal of the individual from:

4.3.1 having access to BT Systems or BT Information; or

4.3.2 carrying out work connected with the provision of the Supplies.

In addition the Supplier should ensure they have relevant processes in place to ensure any Contract Personnel who have been so removed are not subsequently given access to BT Systems, BT Information or allowed to work in connection with the provision of the Supplies.

4.4 The Supplier shall, to the extent permissible by the law, maintain a confidential hotline facility, available to all its personnel, to be used by the Contract Personnel if they are instructed to act in a manner inconsistent or in violation of these Security Requirements. Relevant reports to be notified to the BT Security Contact.

4.5 When Contract Personnel are no longer assigned to the Supplies, the Supplier shall ensure that:

4.5.1 access to BT Information is revoked; and

4.5.2 at BT's option, any BT Physical Assets or BT Information in the possession of Contract Personnel should be either:

4.5.2.1 handed back to the relevant BT operational team; or

4.5.2.2 destroyed in accordance with the most current version of the Third Party Information Classification and Handling Specification.

4.6 Unless otherwise agreed in writing with the BT Security Contact the Supplier shall implement a controlled exit procedure for Contract Personnel which includes the written request to the BT Security Contact for the removal of access to BT Systems, BT Information, and all other Access and accesses. Contract Personnel should be advised that their confidentiality agreement will remain in force and that BT Information acquired through work on the Supplies must not be disclosed.

4.7 As part of the granting of Access the Supplier shall maintain and supply records of all Contract Personnel that require access or are involved in the provision of Supplies to BT, including their name, location they work in, business e-mail address, direct business telephone number and extension (if applicable) and/or mobile number, date User Id Number (UIN) requested (If they have one), date they were assigned to the provision of Supplies to BT , date they completed mandatory training, date they cease providing Supplies and a pre-employment check declaration. It shall be the responsibility of the he Supplier Security Contact to ensure at all time that only Contract Personnel are Authorised.

4.8 The Supplier shall have policies and processes in place to ensure Contract Personnel do not use social media to publish or post online, any statement, commentary, content or images that;

4.8.1 could reasonably be attributed as the views of BT;

4.8.2 release any BT Information that is Confidential Information, or marked as 'In Confidence' or 'In Strictest Confidence'; and

4.8.3 are defamatory to BT, and might cause harm to BTs brand and reputation.

5 AUDIT & SECURITY REVIEW

5.1 Without prejudice to any other right of audit that BT may have, in order to assess the Supplier's compliance of these Security Requirements and where applicable the Condition headed **"Protection of Personal Information"**, BT or its appointed representatives reserves the right to conduct a security compliance audit from time to time, on any or all aspects of the Supplier's policies, processes and system(s) (subject to the Supplier protecting the confidentiality of any information not

related to the provision of the Supplies to BT), by a document based security review or at Supplier's and any relevant Subcontractor's site(s) which are materially involved in the provision of the Supplies or performing the Contract.

5.2 The Supplier will provide BT, or its representatives, access and assistance as necessary and appropriate to allow document based security reviews or on site audits to be undertaken. A minimum of 30 working days' notice will be provided to Supplier prior to a routine onsite audit, however for the avoidance of doubt, in the event of an actual or suspected Personal Data Breach or Relevant Security Breach BT shall not be provided to provide such notice.

5.3 The Supplier will work with BT to implement agreed recommendations and carry out any corrective action BT deems necessary resulting from a document based security review or on site audit within 30 days of being notified of such recommendations or corrective action by BT or such period as agreed between the Parties at the Suppliers expense

5.4 Should BT need to conduct an independent audit of the Supplier and the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001:2013 then Supplier shall, at its own expense, undertake at its own expense those actions required in order to achieve the necessary compliance and shall reimburse in full any costs incurred by BT in obtaining such audit.

6 INVESTIGATION

6.1 If BT has reason to suspect that there has been a:

6.1.1 Personal Data Breach;

6.1.2 Relevant Security Breach;

6.1.3 or a breach of these Security Requirements,

BT shall inform the Supplier Security Contact and the Supplier agrees, at its own cost:

6.1.4 to take action immediately to investigate the suspected breach and to identify, prevent and make reasonable efforts to mitigate the effects of any such breach; and

6.1.5 to carry out any recovery or other action necessary to remedy the breach.

6.1.6 provide to BT such reports as BT shall reasonably require concerning the investigation findings and actions taken to remedy or mitigate the breach,

In the event of a serious breach Supplier shall fully cooperate with BT in any ensuing investigation or audit by BT, a regulatory authority and/or any law enforcement agency, such investigation or audit to include (upon reasonable notice by BT to the Supplier) access to BT Information held within Supplier's premises or on Supplier Systems by

During any investigation, Supplier shall co-operate with BT, by providing access and assistance as necessary and appropriate to investigate the breach. BT may request the Supplier quarantine for evaluation any tangible or intangible asset belonging to Supplier in order to aid the investigation and Supplier shall not unreasonably withhold or delay such request.

PART 4: SPECIFIC SECURITY REQUIREMENTS

7 GENERIC SECURITY REQUIREMENTS & POLICY

7.1 The Supplier warrants and represents that the Suppler Systems, Supplies, associated services, processes and physical locations are compliant with and shall continuously comply with the ISO/IEC 27001:2013 standard and any amended or future version of the standard issued. This compliance must be assured either at, BT's sole discretion by:

7.1.1 certification of the Suppliers ISMS by a UKAS or an international equivalent approved certification body where the scope and statement of applicability has been validated by BT; or

7.1.2 a bi-lateral audit and testing process specified by BT.

7.2 The Supplier must submit a valid the ISO/IEC 27001 certificate at the start of the Contract and on future re-certifications.

7.3 Should the scope of the certificate or statement of applicability be changed at any time, the Supplier must submit these changes for re-validation using the change control procedure (or, in the absence of a change control procedure, through the variation process). The Supplier must inform BT within 2 working days of any major non-conformance identified by the certification body or the Supplier.

8 PHYSICAL SECURITY - BT PREMISES

Compliance with this section is required if Supplier is providing Supplies at a BT premises.

8.1 All Contract Personnel working on BT premises shall be in possession of, and display prominently, an Supplier or BT provided identification card proving the Contract Personnel have been Authorised (the "**Authorised Access Card**"). Authorised Access Cards shall include a photographic image displayed on the card that is clear and be a true likeness of the Contract Personnel. Contract Personnel may also be provided with an electronic access card and/or limited duration visitor card which shall be used in accordance with local issuance instructions.

8.2 Where Contract Personnel have been issued with an Authorised Access Card by BT the Supplier must notify BT promptly and in any event within 5 working days when such Contract Personnel no longer requires access to BT premises.

8.3 Only approved BT build servers, BT Webtop PCs and Trusted End Devices are allowed to directly connect (plug into LAN port or Wireless connection) to BT domains. Supplier shall not (and, where relevant, shall ensure that any Contract Personnel shall not) without the prior written authorisation of the BT Security Contact connect any equipment not approved by BT to any BT Domain. The BT Security Contact shall only provide the written authorisation upon initiating the security policy concession process within BT. In any event Supplier must ensure that no equipment personally owned by Contract Personnel or any other employees, (including contractors, temporary employees and agency workers) is used to store, access or process any BT data.

8.4 No BT Information shall be removed from BT premises and no equipment or software shall be either removed or installed in BT Premises without prior authorisation by BT.

8.5 Physical protection and guidelines for working in BT premises shall be adhered to, and shall include but not be limited to, the escorting of Contract Personnel and the adoption of appropriate working practices within secure areas.

8.6 Where Supplier is authorised to provide its Contract Personnel with un-hosted access to areas within the BT estate; the BT authorised signatory and Contract Personnel must adhere to the guidance document "**Supplier Access To BT's Sites and Buildings**" http://www.selling2bt.com/working/third_party_access/default.htm. Additionally the non BT authorised signatory and Contract Personnel shall have as minimum L2 pre-employment checks http://www.selling2bt.com/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

9 PHYSICAL SECURITY - SUPPLIER PREMISES

Compliance with this section is required if Supplier is providing Supplies from a non-BT premises. (E.g. Suppliers or Supplier's 3rd parties)

9.1 Access to non BT premises (sites, buildings or internal areas) where Supplies are provided, or where BT Information is stored or processed, shall only be permitted using an Authorised Supplier identification card. This card is to be used as a means of identity verification on the applicable premises at all times and as such the photographic image displayed on the card should be clear and be a true likeness of the individual. Individuals may also be provided with an Authorised electronic access card to access the applicable premises or keypad security access. The Supplier must have processes for: authorisation, the dissemination of code changes (which must occur monthly, as a minimum); and ad-hoc code changes.

9.2 Supplier shall ensure that access to non BT premises where Supplies are carried out or; where BT Information is stored or processed, must be authorised and Supplier must adhere to security processes and procedures the control and monitoring of Contract Personnel, visitors and other external persons, including third parties with physical access to these areas (e.g. environmental control maintenance, alarm companies, cleaners).

9.3 If requested by BT, the Supplier shall ensure that Contract Personnel are segregated in a secure manner from all other Supplier personnel. Additionally Supplier must ensure that the systems and infrastructure used to deliver the Supplies are contained within a dedicated logical network. This network must only consist of the systems dedicated to delivery of a secure data processing facility.

9.4 Secure areas in Supplier premises (e.g. network communications rooms), shall be segregated and protected by appropriate entry controls to ensure that only Authorised Contract Personnel are allowed access to these secure areas. The access made to these areas by any Contract Personnel must be audited monthly as a minimum and an assessment of re-authorisation of access rights to these areas must be carried out annually as a minimum.

Evidence of risk assessment will be provided by Supplier to BT on request. Where this is not made available to BT upon request, then at BT's discretion, a risk assessment of the environment used to deliver the Service (such as data centres, data processing areas, computer rooms) will be carried out by BT or its representative prior to commencement of the provision of Supplies. In addition, BT must be informed before any substantial works to any premises that could compromise the security of BT's information.

9.5 CCTV security systems and their associated recording medium shall be used by Supplier either in response to security incidents, as a security surveillance tool, as a deterrent or as an aid to the possible apprehension of individuals caught in the act of committing a crime. Where CCTV images are recorded (either on tape or digitally), they must be retained for a minimum of 20 days. This period may however be extended in the following situations:

9.5.1 where CCTV video evidence has to be retained for an incident or criminal investigation; or

9.5.2 where specified as a necessary requirement to adhere to legislation.

9.5.3 All CCTV recordings must be stored in a locked cabinet and the key securely held and controlled. Access to the cabinet must be restricted to authorised personnel only.

9.6 All CCTV recorders shall be securely located to prevent modification or deletion and the possibility of 'casual' viewing of any associated CCTV screens and in accordance with the guidance on the use of CCTV can be found at

http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm

9.7 All areas of Supplier premises used for the provision of Services and Supplies, shall be inspected for risks and threats at least monthly by the Supplier. The Supplier must have considered and implemented all appropriate measures to ensure physical security with respect to the following:

9.7.1 awareness of local threats including, but not limited to, potential threats from local industry and proximity of stored hazardous materials; and

9.7.2 natural disasters, including risks from threats including, but not confined to flooding, landslip or extreme weather.

9.8 Power and telecommunication cabling within the Supplier's premises carrying data or supporting information services or radio/satellite services used in the provision of the Supplies must be assessed by Supplier for the level of protection to prevent the interruption of business operations. Physical security protection measures commensurate with the business criticality of the operations they serve must be implemented as follows:

9.8.1 business critical carriageway, cable shielding, manholes or footway boxes carrying business critical cables must be protected;

9.8.2 access to cable chambers or cable riser cupboards within operational buildings must be restricted with the use of either electronic access control readers or effective key management;

9.8.3 computer communications links and communications equipment within computer installations must be physically and environmentally protected; and

9.8.4 radio and satellite communications links and communications equipment must be appropriately protected.

9.9 BT shall require, unless otherwise agreed between the Supplier and the BT Security Contact, that manned security services are implemented by the Supplier to complement the electronic and physical security measure at the Supplier's premises where:

9.9.1 location is of operational importance (e.g. contact Centres, data centres, key network sites, etc.)

9.9.2 BT Information processed can impact or be detriment BT's brand and reputation

9.9.3 a high volume of BT information is processed (e.g. business process outsource)

9.9.4 Customer contractual requirements

9.9.5 there is a site specific risk/threat

9.9.6 Supplier is in possession of BT information that has a high level of sensitivity.

9.10 To protect BT equipment (such as servers or BT switches) on the Supplier's premises from environmental threats or dangers, and from the possibility of unauthorised access; BT Equipment must be sited in a protected area and segregated from equipment used for any non-BT organisations systems. The level of segregation should ensure that the security of BT equipment cannot be compromised either deliberately or accidentally as a result of access granted to non-BT organisations and could for example take the form of secure partition walling, lockable cabinets or metal caging.

9.11 Supplier must have implemented appropriate measures to ensure physical security with respect to the following:

9.11.1 fire prevention measures including but not limited to alarms, detection and suppression equipment;

9.11.2 climatic conditions, with consideration given to temperature, humidity and static electricity and the associated management, monitoring and response to extreme conditions (such as automatic shutdown, alarms);

9.11.3 control equipment including, but not limited to air conditioning and water detection;

9.11.4 location of water tanks, pipes etc. within the premises;

9.11.5 auditable access – where appropriate access to systems by personnel must be auditable; and

9.11.6 supervision of Contract Personnel not normally associated with the management of or Access to, BT's systems.

9.12 Security perimeters (barriers such as walls, fences, card controlled entry gates or manned reception desks) shall be used to protect areas that contain sensitive BT information or BT Customer information (including Personal Data) and associated processing facilities.

9.13 Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access or deliberate attacks.

9.14 Supplier shall ensure that physical access to areas that have Access to BT Information or BT Customer information (including Personal Data) is with smart or proximity cards (or equivalent security systems) and Supplier must conduct monthly internal audits as a minimum to ensure compliance with these provisions.

9.15 Supplier shall ensure that photography and/or the image capture of any BT Information or BT Customer information (including Personal Data) is prohibited. Under exceptional circumstances where there may be business requirements to capture such images, temporary exemption to this provision must be obtained in writing from the BT Security Contact.

9.16 Supplier shall maintain a clear-desk and a clear-screen policy to protect BT Information.

10 PROVISION OF HOSTING ENVIRONMENT

Compliance with this section is required if the Supplier is providing a hosting environment for BT or BT Customer equipment.

10.1 The Supplier shall, where the Supplier is providing a secure access area on their premises for hosting BT or BT Customer equipment ("**Supplier Site**"):

10.1.1 ensure that all Contract Personnel accessing the Supplier Site are in possession of an identification card or electronic access control card. This card is to be used as a means of identity verification on the Supplier Site at all times and as such the photographic image displayed on the card should be clear and be a true likeness of the Contract Personnel; and

10.1.2 have implemented procedures to deal with security threats directed against BT's or BT's customer's equipment or against a third party working on behalf of BT in order to safeguard BT's and BT's customer's Information at the Supplier Site; and

10.1.3 use CCTV security systems and their associated recording medium at the Supplier Site in response to security incidents, as a security surveillance tool, as a deterrent and as an aid to the possible apprehension of individuals caught in the act of committing a crime. The Supplier shall ensure that 20 days of CCTV is recorded to be effective as an investigative tool; and

10.1.4 provide BT with a floor plan of allocated space in the secure area of the Supplier Site; and

10.1.5 ensure that BT's and BT's customer's cabinets at the Suppliers Site are kept locked and only accessed by authorised BT personnel, BT's approved representatives and relevant Contract Personnel; and

10.1.6 implement a secure key management process at the Supplier Site; and

10.1.7 inspect the local area surrounding the Supplier Site for risks and threats on a regular basis; and

10.1.8 document and maintain operating procedures (in the language of the country originating the BT work) to discharge the security requirements detailed within this paragraph 10 and on request provide BT with access to such documentation.

10.2 BT shall provide the Supplier with:

10.2.1 a record of BT's and/or BT's customer's physical assets held at the Supplier Site; and

10.2.2 details of BT's employees, subcontractors and agents that need access to the Supplier Site (on an on-going basis).

11 DEVELOPMENT OF SERVICES

Compliance with this section is required if Supplier is dealing with the development of Supplies for use by BT and/or BT Customers. This includes "components off the shelf", configuration of software and manufacturing components for the Supplies.

11.1 Supplier shall, implement agreed security measures across all supplied components that constitute the Supplies and/or Services, such that it safe guards the confidentiality, availability and integrity of the Supplies, including by:

11.1.1 maintaining appropriate documentation (in the language of the country originating the BT work) in relation to the implementation of security and shall ensure that it and such security, is in accordance with best industry practice;

11.1.2 minimising the opportunity for unauthorised individuals (e.g. hackers) to gain access to BT Systems and BT Information, BT Networks or BT Supplies; and

11.1.3 minimising the risk of misuse of BT Systems and BT Information, BT Networks or the Services which could potentially cause loss of revenue or service.

11.2 Supplier shall demonstrate, on request, that any supplied software or hardware build (both proprietary and off-the-shelf) delivered to BT is the same as that agreed with BT. Supplier shall maintain integrity of builds including upgrades, operating systems and application from factory to desk.

11.3 Supplier shall ensure that the development of systems for use by BT or the build and maintenance of BT owned hardware is hardened to BT's IT Security Requirements if provided by the BT operational team or developed to best industry practice.

11.4 Supplier shall ensure that systems and processes used for test and development activities are segregated from production systems. A change control process must be used for the promotion of any code to the production environment. BT provided

test data must be deleted after a period determined by the BT data owner and no live or production data can be used in development or test environments.

11.5 All critical security vulnerabilities found in security testing and classified as medium risk or above must be fixed prior to release. Any security weaknesses in the Services identified by BT or the Supplier shall be remedied at the Supplier's cost within such timescales as BT shall reasonably require.

11.6 The Supplies must be subject to independent penetration testing commissioned by the Supplier prior to release, on at least an annual basis and following major changes or incidents at Supplier's own cost.

11.7 Supplies developed for use by BT or its customers must be developed using a documented, recognised industry standard Secure Development LifeCycle (SDLC) to minimise the risk of introducing security vulnerabilities into the production environment and/or to customers. The SDLC must include the following gates, with tangible artefacts resulting from each review and available for inspection by BT within the audit framework at paragraph 5 of Part 3 of these Security Requirements:

11.7.1 security review of the business requirements;

11.7.2 security review of the design;

11.7.3 security review of the source code – automatic and/or manual; and

11.7.4 security audit of the solution prior to deployment (to include simulated attacks) according to a documented, project-specific audit plan based on the reports resulting from the security reviews of business requirements, design and code.

Further guidance can be found in Third Party-Industry Guidance Standards on 'Secure Coding':

http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm

12 ESCROW

Now contained within main contract.

13 ACCESS TO BT SYSTEMS

Compliance with this section is required if Supplier Contract Personnel need to access BT Systems in order to provide Supplies.

13.1 BT may allow, at is sole discretion, limited Access as is strictly necessary for the provision of Supplies.

13.2 In relation to Access, Supplier shall adhere to all relevant BT policies, standards and instructions provided to Supplier, and shall (and, will ensure that all Contract Personnel shall):

13.2.1 ensure user identification, passwords, PINs, tokens, and conferencing access are for individual Contract Personnel and not shared. Details must be stored securely and separately from the device they are used to access. If a password is known by another person it must be changed immediately;

13.2.2 on reasonable request, provide to BT such reports as BT shall reasonably require concerning Contract Personnel Authorised to access BT Systems;

13.2.3 inter domain linking to BT Systems is not permissible unless specifically approved and authorised by BT Security Contact;

13.2.4 use all reasonable endeavours to ensure no viruses or malicious codes (as the expressions are generally understood in the computing industry) are introduced to minimise risk of corruption to BT Systems or BT Information through any means whatsoever; and

13.2.5 use reasonable endeavours to ensure that files which contain information, data or media with no relevance to the Supplies are not stored on BT Equipment, BT servers, BT provided laptops and desktops, BT centralised storage facilities or BT Systems.

13.2.6 where BT has provided Supplier with access to the internet or BT's intranet, ensure that the Contract Personnel only access the internet or BT intranet appropriately and only enable them to provide the applicable Supplies and that [unacceptable or dangerous sites should be blocked from the user . It is the Supplier's responsibility to ensure that guidance on internet and email abuse is communicated to the Contract Personnel as a minimum annually. This guidance must require that:

13.2.6.1 users shall not:

(a) Access any offensive, sexual, sexist, racist or politically offensive content;
(b) Carry out any acts that may bring BT or individuals into disrepute;
(c) running a private business;
(d) infringe any copyright or;

(e) bypass or tunnel through BT's firewall or other security mechanisms;

13.2.6.2 Contract Personnel do not contribute to sites or post online statements that could be reasonably attributed as the views of BT.

13.3 The Supplier must carry out regular reviews to ensure that Access is required to perform the role. Copies of review documentation must be made available for inspection by BT within the audit framework described in paragraph 5.1:

13.4 The Supplier must notify BT promptly and in any event within 5 working days when an employee, including contractors, temporary employees and agency workers, no longer require Access to BT systems, for example when employees leave or move roles.

14 ACCESS TO BT INFORMATION ON SUPPLIER SYSTEMS

Compliance with this section is required if BT Information is being stored or processed on Supplier Systems.

14.1 If Contract Personnel are granted Access to Supplier Systems for the purpose of providing the Supplies and/or Services, the Supplier shall demonstrate accountability for such Access (including, but not limited to the use of unique user accounts, password management and a clear audit/log trail for all Contract Personnel action

14.2 Supplier shall maintain systems which detect and record any attempted damage, modification or un-authorised access to BT Information on Supplier Systems. Examples, include but not limited to system logging and auditing processes, IDS and IPS etc.

14.3 Supplier shall maintain controls to detect and protect against malicious software, viruses and malicious codes on Supplier Systems and ensure that appropriate user awareness procedures are implemented.

14.4 Supplier shall ensure that any unauthorised software is identified and removed from Supplier Systems holding, processing or accessing BT Information at least monthly.

14.5 Supplier shall ensure that access to diagnostic and management ports as well as diagnostic tools are securely controlled.

14.6 Supplier shall ensure that access to Supplier's audit tools are restricted to Contract Personnel and their use is monitored.

14.7 Supplier shall ensure code reviews and penetration testing on all in-house produced software (including any Software) used to process BT Information is performed by an independent team that must not include the developers of the software.

14.8 To the extent that any servers are used to provide the Supplies, they must not be deployed on un-trusted networks (network's outside your security perimeter, that are beyond your administrative control e.g., internet-facing) without appropriate security controls.

14.9 Supplier shall ensure that changes to individual Supplier Systems which hold and process BT Information and/or which are used to provide the Supplies, are controlled and subject to formal change control procedures.

14.10 Supplier shall ensure that all system clocks and times are synchronised using the latest version of NTP or a similar time synchronisation technology.

14.11 Where Supplier provides systems that enable online access for BT Customers:

14.11.1 Online credentials for BT Customers must contains the following as a minimum:

14.11.1.1 user ID;

14.11.1.2 online password;

14.11.1.3 three authentication questions and answers to support account access; and

14.11.1.4 an alternate method of contact for authentication purposes.

14.11.2 The BT Customer must be able to choose a unique User ID for their online credentials and online password must not contain their unique User ID.

14.11.3 The BT Customer's online password must be a minimum length of 8 characters and contain at least 1 character from 3 of the following sets; (i) decimal number (0-9),(ii) capital case letter (A-Z), (iii) lower case letter (a- z) (iv) non alpha-numeric

14.11.4 To change an online password the BT Customer must provide their current password followed by double entry of the new password.

14.11.5 When a BT Customer User-ID or password is forgotten, the system provided by the Supplier must generate an email to the registered email address of the BT Customer containing the User-ID or password reset request link after successful entry on the online form of the following:

14.11.5.1 MSISDN or Landline number

14.11.5.2 Online password

14.11.5.3 BT Customer User ID

14.11.6 The password reset request link must have a limited duration of validity of 30 minutes maximum, before it expires and a new reset of online password request has to be made.

14.11.7 On successful password reset, the BT Customer must be forced to change to a new password.

14.11.8 Recovery of BT Customer user credentials when the both the User ID and online password is forgotten must generate an email to the registered email address containing the User ID and a password reset request link after successful entry of the first name and last name, phone number and email address of the BT Customer.

14.11.9 Additional levels of customer authentication may be required based on the sensitivity of the data and functionality to be accessed.

15 SUPPLIER HOSTING BT INFORMATION

Compliance with this section is required where Supplier is externally hosting BT Information classified as "In Confidence" or "In Strictest Confidence" in a cloud services environment or in Suppliers or Subcontractors server environment.

15.1 The Supplier shall, in relation to the Supplies, ensure that environments where BT Information is hosted comply with the 3rd Party External Data Hosting Requirements available at: http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm.

16 NETWORK SECURITY

Compliance with this section is required where the Supplier is building, developing or supporting BT Networks or Network Assets.

16.1 The Supplier shall, in relation to the Supplies, implement agreed security measures across all supplied components, such that it safeguards the confidentiality, availability and integrity of the BT Networks and/or 21CN assets. The Supplier shall provide BT with full documentation in relation to the implementation of Network Security in relation to the Supplies and shall ensure that it:

16.1.1 meets, and ensure that all Network Security for which the Supplier is responsible meets all legal and regulatory requirements; and

16.1.2 uses its best endeavours to prevent unauthorised individuals (e.g. hackers) from gaining access to the Network Management Elements and other elements accessed via the BT Networks and/or 21CN; and

16.1.3 uses its best endeavours to reduce the risk of misuse of the BT Networks and/or 21CN by those individuals authorised to access it,, which could potentially cause loss of revenue or service; and

16.1.4 uses its best endeavours to detect any security breaches that might occur ensuring quick rectification of any breaches, alongside the that result and identification of the individuals who obtained access and determination of how they obtained it; and

16.1.5 minimise the risk of misconfiguration of BT Networks for example by granting the minimum permissions required to fulfil the contracted role.

16.2 The Supplier must take all reasonable steps to secure all interfaces on the Supplies and/or Services, and should not assume that the supplied components are operated in a secure environment.

16.3 The Supplier shall provide to the BT Security Contact the names, addresses (and such other details as BT shall require) of all individual Contract Personnel who shall from time to time be directly involved in the deployment, maintenance and/or management of the Supplies before they are respectively engaged in such deployment, maintenance and/or management.

16.4 In relation to its UK-based support activities, the Supplier shall retain a skilled security team comprised of at least one UK national who shall be available for liaison with the BT Security Contact (or his nominees) and the team shall attend such meetings as the BT Security Contact shall from time to time reasonably require.

16.5 The Supplier shall provide the BT Security Contact with a schedule (updated as necessary from time) of all active components comprised in the Supplies and/or the Services and their respective sources.

16.6 The Supplier shall provide details of its individual personnel who will liaise with the BT vulnerability management (CERT) team in relation to discussion around BT and Supplier-identified vulnerabilities in the Supplies and/or Services. The Supplier shall provide BT with timely information on vulnerabilities, and comply(at the Supplier's cost) with such reasonable requirements in relation to vulnerabilities as may be notified by the BT Security Contact from time to time. The Supplier shall inform BT of any vulnerabilities in sufficient time to allow mitigating controls to be i applied or installed ahead of the Supplier releasing the vulnerabilities publicly.

16.7 The Supplier shall permit the BT Security Contact and his nominees from time to time full and unrestricted access to any premises where the Supplies are developed, manufactured, or created to perform security compliance testing and/or

assessments, and the Supplier shall co-operate (and shall ensure that all relevant Contract Personnel co-operate) in such security compliance testing.

16.8 The Supplier shall ensure that any security-related components comprised in the Supplies as are identified by or to BT from time to time are, at the Supplier's cost, externally evaluated to BT's reasonable satisfaction.

16.9 In relation to any Information provided by or obtained from BT that is marked "**IN STRICTEST CONFIDENCE**" or easily interpreted to be deemed confidential, the Supplier shall ensure that:

16.9.1 access to it is given only to those Contract Personnel specifically authorised by BT to view and handle it and a record kept of such access;

16.9.2 it is handled, used and stored with great care and encrypted prior to storage using PGP or WinZip 9, and under conditions which offer a high degree of resistance to deliberate compromise (i.e. using the strongest available encryption algorithm / using a strong password) and which make actual or attempted compromise very likely to be detected;

16.9.3 when it is transmitted, adequate security is applied to it by encrypting with Secure Email, PGP or WinZip 9; and

16.9.4 it is not, without BT's written permission, exported outside the European Economic Area.

16.10 The Supplier shall promptly, and in any event within 7 Working Days, provide to the BT Security Contact full details of any features and/or functionality in any the Supplies (or that are planned in the Roadmap for any the Supplies) that from time to time:

16.10.1 the Supplier knows; or

16.10.2 the BT Security Contact reasonably believes and so informs the Supplier are designed for, or could be used for, lawful interception or any other interception of telecommunications traffic. Such details shall include all Information that is reasonably necessary to enable the BT Security Contact to fully understand the nature, composition and extent of such features and/or functionality.

16.11 In order to maintain access to BT Networks and/or systems, Supplier shall notify BT immediately of any changes to its Access method through the firewalls, including the provision of network address translation.

16.12 The Supplier must not use any network monitoring tools that can view application information.

16.13 The Supplier shall ensure that IPv6 functionality included in operating systems is disabled on hosts (for example end user devices or servers) that connect to the BT Network and domains should be disabled where not required.

16.14 Supplier shall comply and shall ensure that the Supplies or Services comply with BT policies where provided and the Security Requirements. Any non-compliance must be agreed at contract signature or through a change control (or equivalent) process.

16.15 The Supplier shall ensure that all Contract Personnel have pre-employment checks appropriate to the level of Access as set out at http://www.selling2bt.com/Downloads/3rdPartyPECsPolicy-v1.1.pdf.

Suppliers building, developing or supporting BT Networks or Network Assets shall ensure that all Contract Personnel have as minimum L2 pre-employment checks. L3 pre-employment checks will be required for roles identified by the BT Security Contact. Where the Supplier does not have the capability to directly security clear Contract Personnel as part of L3 checks then BT will assist in obtaining clearance at the Supplier's cost.

16.16 Supplier shall maintain hardware and software according to manufacturers' specifications.

16.17 Supplier shall not use removable media (disks, USB drives, etc.) intended for support and maintenance for any other purpose.

17 SUPPLIER NETWORK SECURITY

Compliance to the clauses in this section is required where the supplier's network will be utilised in order to provide the supplies (this includes, LAN, WAN, internet, wireless and radio networks).

17.1 The Supplier shall, in relation to the Supplies or Services, implement security measures across their networks, such that it safeguards the confidentiality, availability and integrity of BT Information. The measures shall and the Supplier shall:

17.1.1 meet all legal and regulatory requirements; and

17.1.2 use its best endeavours to prevent unauthorised individuals (e.g. hackers) from gaining access to the Supplier Network(s);

17.1.3 use its best endeavours to reduce the risk of misuse of the Supplier Network (s) by those individuals authorised to access it, which could potentially cause loss of revenue or service and

17.1.4 use its best endeavours to detect any Relevant Security Breaches and ensure quick rectification of any breaches, alongside the identification of the individuals who obtained access and determination of how they obtained it.

17.2 Appropriate measures must be in place to ensure the security of components including but not limited to:

17.2.1 use of effective "defence in depth" principles;

17.2.2 use of controls in place that prevent any purposeful attack;

17.2.3 use of firewalls, routers, switches;

17.2.4 secure communications between devices and management stations;

17.2.5 secure communications between devices as appropriate; including the encryption of all non-console administrator access;

17.2.6 strong architectural design, which are tiered and zoned with effective robust identity management and operating system configuration which must be appropriately hardened and documented;

17.2.7 the disabling (where practical) of services, applications and ports that will not be used.

17.2.8 the disabling or removal of guest accounts.

17.2.9 the installation of the most recent security patches on the Supplier's Network(s) and system(s) as soon as practicable following testing. Any exceptions must be communicated to BT where such exceptions will be risk assessed. BT reserves the right to obligate Supplier to install patches following risk assessment;

17.2.10 the avoidance of trust relationships between servers;

17.2.11 use of the best practice security principle of "least privilege" to perform a function;

17.2.12 ensuring appropriate measures are in place to handle denial of service attacks;

17.2.13 ensuring appropriate measures are in place for intrusion detection and/or protection;

17.2.14 monitoring all applicable vendors and other relevant information sources for vulnerability alerts;

17.2.15 where appropriate, filing integrity monitoring to detect any additions, modifications or deletions of critical system files or data; and

17.2.16 change all default and vendor supplied passwords before network components go live.

18 CLOUD SECURITY

Compliance to the clauses in this section is required when the Supplier is providing BT with Cloud services.

18.1 The Supplier shall comply with:

the latest version of the Cloud Security Alliance Cloud Controls Matrix (CCM); BT's External Hosting Security requirements available at: http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer requirements.

18.2 Supplier shall, implement agreed security measures across all supplied components, such that it safeguards the confidentiality, availability, quality and integrity of the Supplies by minimizing the opportunity of unauthorised individuals (e.g. other cloud customers) from gaining access to BT Information, and BT Supplies.

19 CONTACT CENTRE

Compliance with clauses in this section is required where Supplier is providing a contact centre for BT.

19.1 The Supplier shall, in relation to the Supplies, ensure that environments where BT Information is stored, processed or viewed comply with the most current version of the Contact Centre 3rd Party Standard available at: http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm.

PART 5: DEFINITIONS

In these Security Requirements, the following definitions will apply, but otherwise the terms of the Contract shall apply to these Security Requirements and all words and expressions used in these Security Requirements shall bear the same meaning given to them in the Contract:

"**Access**" – the Processing, handling or storing BT Information by one or more of the following methods:

- By interconnection with BT Systems
- Provided in paper or non-electronic format
- BT Information on Supplier Systems
- by mobile media

and/or access to BT premises for the provision of the Supplies excluding the delivery of hardware and meeting attendance).

"**Authorised**" - BT has approved Access either as part of BT's System Interconnect process or written authorisation has been received from the BT Security Contract "**authorisation**" shall be construed accordingly. Access level provided will be relevant and limited to that required to provide the Supplies.

"**BT's Administrative Systems**" – shall mean BT invoicing platform (currently iSupplier), or such other systems as agreed with BT are purely administrative;

"**BT Customer**" – shall include for the purposes of these Security Requirements a corporate or individual to whom BT provides goods or services.

"**BT Information**" – all Information relating to BT or a BT Customer provided to the Supplier and all Information which is processed or handled by the Supplier on behalf BT or a BT Customer pursuant to the Contract.

"**BT Networks**" - the network controlled or administered by BT.

"**BT Physical Assets**" - all physical assets (including but not limited to routers, switches, servers keys to cabinets, laptops tokens, pass cards, plans, or documentation) held by Supplier which belong to BT.

"**BT Security**" - the security organisation based within BT.

"**BT Security Contact**" – the information assurance professional within BT Security or Commercial BT Contact if notified to the Supplier or central Security 0800 321999 [+44 1908 641100] who will be the single point of contact for issues related to these Security Requirements and any Relevant Security Incident.

"**BT Systems**" – the services and service components, products, networks, servers, processes, paper based system or IT systems (in whole or part) owned and/or operated by BT or such other systems that may be hosted on BT Premises including iSupplier (as is defined in the Condition headed "**Payment and Invoicing**").

"**Bulk Records**" – means more than 1000 individual records of BT Information classified as In Confidence or 100 individual records of BT Information classified as In Strictest Confidence.

"**CCTV**" - close circuit television.

"**Contract Personnel**" "**Relevant Contract Personnel"** - as defined in the contract.

"**Cyber Essentials Plus**" – means UK Government backed scheme to help organisations protect themselves against common cyber-attacks currently available at https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

"**Good Industry Security Practices**" – means in relation to any undertaking and any circumstances, the implementation of the security practices, policies, standards and tooling which would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same type of activity under the same or similar circumstances.

"**Information**" – information whether in tangible or any other form, including, without limitation, specifications, reports, data, notes, documentation, drawings, software, computer outputs, designs, circuit diagrams, models, patterns, samples, inventions, (whether capable of being patented or not) and know-how, and the media (if any) upon which such information is supplied.

"Internal", "Public", "**In Confidence**" and "**In Strictest Confidence**" – have the meanings given to them in the Third Party Information Classification and Handling Specification.

"**ISO 27001**" – the current version of the international standard for international security management systems set by the International Organisation for Standardization and the International Electrotechnical Commission.

"**Network Assets**"- device, or other component of the BT Network that supports network related activities.

"**Network Security**" - the security of the interconnecting communication paths and nodes that logically connect end user technologies together and associated management systems.

"**Process**", "**Processed**" or "**Processing**" "**Processing Appendix**" and "**Personal Data**" - shall have the meanings ascribed to them in the Condition headed "**Protection of Personal Data**".

"Relevant Security Incident" - an observed or suspected security weaknesses in systems or services, and security events that affect the Supplies or the performance of the Contract (including actual or suspected loss, damage, theft or misuse of BT Information or BT Systems), including but not limited to:

- loss of service, equipment or facilities;
- corruption, damage or misuse of BT Physical Assets;
- system malfunctions or overloads;
- human errors;
- non-compliances with the security requirements described in this document;
- breaches of physical security arrangements;
- uncontrolled system changes;
- malfunctions of software or hardware;
- access violations; and
- known or suspected data losses related to systems associated with BT and the connection(s) between BT and Supplier.

"Remote Access" - remote access from home or another location via a public network (e.g. Internet)
or Supplier network remotely access a BT System.

"Security Requirements" - means these BT security requirements as duly updated from time to time.

"**Supplies**" – shall mean any and all of the "Services", "Supplies" "Goods" and "Work" defined in the Contract and any performance of the Contract.

"**Supplier Systems**" – any Supplier owned computer, application or network systems used for accessing, storing or processing BT Information or involved in the provision of the Supplies.

"**Supplier Security Contact**" – such person whose contact information shall be notified by Supplier to BT from time to time who will be the single point of contact for issues related to these Security Requirements and any Relevant Security Incident.

"**Transfer**" or "**Transferred**" - the moving of BT Information in the possession of Contract Personnel (including, without limitation, Personal Data) from one location or person to another, whether by physical, voice or electronic means; and granting of Access to BT Information in the possession of Contract Personnel (including, without limitation, Personal Data) by one location or person to another, whether by physical, voice or electronic means.

"Third Party Information Classification and Handling Specification" means the requirements on the Supplier's handling of information as set out at http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm as updated from time to time.