## Table of Contents

# 1. Introduction and Scope

1.1 This document represents BT's baseline security requirements relevant to the scope of work being undertaken by a Supplier. These requirements are in 3 levels.

The 1st level of requirements in section 2 relates to Suppliers who will be performing work that has limited BT Information and may have limited access to BT's administrative Systems and BT Networks, Suppliers who fall into this category will not be required to comply with any other requirements in this document.

The 2nd level sections 3 -6, are mandatory for all other types of work.

For the 3rd level depending on the scope of work one or more requirements in sections 7-18 may be applicable, your BT Procurement representative will be able to advise.

Some of the requirements may reference an Annex as listed below which provides additional information. :

Annex 1 Information Classification
Annex 2 Mandatory Training
Annex 3 Passing queries/Issues to a BT Security Contact
Annex 4 Access to BT Sites and Buildings by non BT Organisations
Annex 5 External Hosting Security requirements

1.2 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 Pre-employment Checks (PECs)).

# 2. Security of Information for Limited Access

**Compliance to Section 2 is the only requirement applicable if Supplier is performing work that has limited access to BT Information and may have limited access to BT's administrative Systems e.g. iSupplier and BT Networks (types of work include but are not limited to stationery, building facilities management, site surveys, voucher schemes and employee discount products, BT TV Content providers and Rights Holders.)**

Without prejudice to any obligations of confidentiality it may have, where the Supplier or Contract Personnel have access to BT's or BT's customer's Information (including personal data) relating to BT or BT's Customers, the Supplier shall:
(a) ensure such Information (including personal data) is not disclosed to or accessed by Contract Personnel not directly employed on BT work and
(b) keep (and ensure all relevant Contract Personnel keep) such Information (including personal data) secure and confidential (including, without limitation, by effecting such systems and procedures as are required to protect the security of all information belonging to or controlled by BT to the extent that it is in the possession or under the control of the Supplier in accordance with industry best practice and implement all such systems and processes rigorously).

## Sections 3 - 6 inclusive are applicable to all supplier engagements with BT (with the exception of those suppliers just providing Limited Access Supplies)

# 3. General Information Security

3.1 Supplier shall promptly notify BT of the Supplier's Security Contact details and any change to them.

3.2 At commencement of the Contract the Supplier shall notify the BT Security Contact in writing using Annex 3 of the geographical locations where the main services are delivered relevant Contract Personnel are located or BT information is processed or stored. During the Contract the Supplier must also notify any proposed change of geographical location to the BT Security Contact via Annex 3, so BT may re-assess any risk to BT or BT Customer Information.

3.3 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.

3.4 The Supplier shall not use BT Information for any purpose other than for the purpose for which the BT Information was provided to the Supplier by BT and then only to the extent necessary to enable the Supplier to perform the Contract. Supplier shall handle or use BT Information in a manner that is consistent with the requirements in Annex 1 of these Security Requirements and in accordance with relevant legislation

3.5 Supplier shall notify BT Security contact using Annex 3, should the supplier be subject to a merger, acquisition, or changes in ownership, so BT may re-assess any risk to BT and BT or BT Customer information.

3.6 Supplier shall as a minimum annually or when there are any changes to the Supplies or how they are provided, review these Security Requirements to ensure they are complying with all applicable Security Requirements.

3.7 Supplier shall securely manage any BT Physical Assets and/or BT Items assigned to the Supplier by BT.

- BT Physical Assets and BT Items shall be securely stored when not in use. Examples include but are not limited to remote access tokens, BT laptops, network equipment, servers and documentation.
- BT Physical Assets shall not be taken off-site from place of work without prior authorisation.

3.8 Supplier shall have in relation to the provision of the Supplies, formal security incident management procedures with defined responsibilities and any information on any security incident shall be treated "In Confidence". Supplier shall inform BT Security Contact using Annex 3, within a reasonable period of time upon its becoming aware of any incident:

i) involving material loss, corruption, damage or misuse of BT Information, BT Physical Assets, BT Items or improper or un-authorised access to BT Systems and BT Information or breach of any of Supplier's obligations under these Security Requirements; or
ii) involving any inability to deliver the Supplies in accordance with the contract.
Iii) any action that is in breach of the requirements in this Security document.

Upon reasonable request, Supplier shall promptly provide to BT a written report with a remedial plan including a timetable and steps to be taken to avoid a repeat of the incident.

3.9 Supplier shall ensure that identified risks to the confidentiality, integrity or availability of BT Information in Supplier's processes or Supplier Systems, are promptly treated

3.10 BT may carry out risk assessments on any relevant part of the service, (which may include subcontractors relevant to the service) to identify additional risks to BT as a result of the provision of the Supplies, as applicable. BT may then stipulate additional countermeasures to address any risks. Any costs associated with the implementation of countermeasures to be agreed by both parties.

3.11 Supplier shall have security policies and processes and maintain documentation (copies to be made available in English) to show compliance with these Security Requirements and provide BT with access to evidence in accordance with Section 7 below.

3.12 Supplier shall ensure procedures and controls are in place to protect the Transfer of BT Information through the use of emails, voice, facsimile and video communications facilities.(E.g. when on conference calls ensure all individuals on the call are authorised to discuss BT Information) For further information on handling BT information see Annex1.

3.13 Supplier shall have implemented procedures to deal with security threats directed or targeted at BT or against a third party working on behalf of BT in order to adequately protect BT Information.

3.14 Supplier shall ensure that remote and home working activities with respect to BT Information and BT Systems are subject to appropriate security controls within Supplier's organisation, including but not limited to remote access by users being subject to strong authentication.

3.15 On termination or the expiration of the Contract, Supplier shall, and shall procure that any Contract Personnel and Subcontractors, securely destroy in accordance with Annex 1 of these Security Requirements any BT Information held or controlled by Supplier or its Subcontractors, unless specified by BT, or required under any legal or regulatory obligations. Archived information must be put beyond use of daily business activities.

3.16 Supplier should keep BT information for as long as necessary to perform the service but no longer than a maximum of two years unless a different retention period has been specified by BT or is required to meet with Legal or regulatory requirements.

3.17 The Supplier shall ensure the availability, quality, integrity and adequate capacity to deliver the required system performance or Supplies with availability without interruption by ensuring:-

- A backup plan is in place
- The critical system data is protected if applicable
- Fall-back is implemented where it is an agreed requirement
- The system or service is recoverable following a major failure or disaster
- The plan is practiced at least annually
- Back-up copies of information and software where applicable shall be taken and tested regularly in accordance with an agreed backup policy to ensure restoration of data without alteration.

## 4. Contract Personnel Security

4.1 Relevant Contract Personnel shall not be granted Access until they have completed BT's Security training as detailed in Annex 2 of these Security Requirements. BT's Security of Information training may be substituted by suppliers own equivalent security of information training subject to approval by BT Security. Thereon mandatory training must be refreshed as detailed in Annex 2. Supplier shall maintain the records of training which shall be made available for audit by BT.

4.2 Supplier shall ensure that all Contract Personnel sign Suppliers confidentiality agreement before they 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 review by BT during audit.

4.3 Supplier shall deal with breaches of security policies and procedures, through formal processes including disciplinary action as appropriate.

4.4 Supplier shall maintain a confidential hotline facility, available to all its personnel, to the extent permissible by the law to be used by the Contract Personnel if they are instructed to act in an inconsistent manner in violation of these Security Requirements. Relevant reports to be notified to the BT Security contact using Annex 3.

4.5 When Contract Personnel are no longer assigned to the Supplies, Supplier shall ensure that access to BT Information is revoked and any BT assets or BT Items or BT Information in the possession of Contract Personnel are handed back to the relevant BT operational team or destroyed in accordance with Annex 1 of these Security Requirements. Where applicable the Supplier shall implement a controlled exit procedure which includes written request to BT Operational lead for removal of BT accesses and Identity. Contract Personnel should be advised that the signed confidentiality agreement is still in force and that BT information acquired through work on the Supplies must not be disclosed.

4.6 As part of the granting of Access the Supplier shall maintain and supply records of all Contract Personnel that need access or are providing BT Supplies including name, location they work in, business e-mail address and 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 BT project, date they completed mandatory training, date they left BT project and a Pre-employment check declaration. Supplier Security Contact shall at all times ensure that only Relevant Contract Personnel are Authorised.

## 5. Audit & Security Review

5.1 Supplier shall, in relation to the Supplies and subject to the Supplier maintaining the confidentiality of information relating to its other clients, allow on reasonable request (and ensure that all Contract Personnel allow) BT or its authorised representatives such access to Supplier's and any relevant Subcontractor's premises, systems and records containing BT and BT Customer Information (including personal data) as is reasonably necessary to assess the Supplier's compliance of these Security Requirements.

This may include assessments of all elements of physical and logical controls and validation of Supplier Systems holding BT Information. Supplier shall facilitate this assessment by permitting BT to collect, retain and analyse information relating to the provision of the Supplies, as applicable, to identify potential security risks; and provide such reports to BT and attend such meetings as may be reasonably required by BT.

If required by BT, Supplier will participate in a remote on-line health check to establish basic security compliance with the security clauses in these Security Requirements.

## 6. Investigation

6.1 If BT has reason to suspect that there has been a breach by Supplier or any subcontractor of the provisions of these Security Requirements, which impact BT Systems and/or BT Information, BT shall inform Supplier Security Contact. Supplier shall cooperate with BT fully in any ensuing investigation by BT and/or any law enforcement agency, which may include access to BT Information in Supplier's premises, by providing reasonable notice to the Supplier.

During investigation, Supplier shall co-operate with BT, providing reasonable assistance and facilities necessary to investigate the breach. BT may request that Supplier shall quarantine for evaluation any tangible or intangible asset belonging to Supplier to aid the investigation and Supplier shall not unreasonably withhold or delay the request.

**For clause sections 7 -18, the description for each section specifies what sort of Supplies the clauses apply to.**

## 7. Generic Security Requirements & Policy

**Compliance to Section 7 clauses is required if Supplier has access to "Sensitive Information" (As per defined term), or is providing development, installation, maintenance, support of network functions or IT Professional services.**

7.1 Supplier shall be ISO27001 certified or shall comply with the Security Requirements of ISO27001 certification or security policies aligned to ISO27001 and/or working towards ISO27001 within a timeframe agreed with BT.

7.2 If provided BT may update from time to time, security related policies, guidelines, security requirements and other requirements. BT shall incorporate relevant updates within an updated version of these Security Requirements by contract change request, which shall be notified in writing by BT to the Supplier. Any costs associated with the implementation of new security requirements to be agreed by both parties.

7.3 Supplier shall make available to BT copies of Security Certifications and statement of applicability relevant to the services being provided to support evidence of compliance to this schedule

## 8. Physical Security - BT Premises

**Compliance to Section 8 clauses is required if Supplier is providing Supplies at BT Premises.**

8.1 All Contract Personnel working on BT premises shall be in possession of an Authorised Supplier or BT provided identification card. This card is to be used as a means of identity verification on BT premises at all times and shall include a photographic image displayed on the card that must be 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 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 (Using annex 3) connect any equipment not approved by BT to any BT Domain. The BT Security Contact shall provide the written authorisation upon initiating the security policy concession process within BT.

8.3 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.

8.4 Physical protection and guidelines for working in BT Premises shall be adhered to e.g. escorting when going to secure areas. Additionally orders or instructions BT gives to the Supplier's Representative shall be deemed to have been given to the Supplier.

8.5 Where Supplier is authorised to provide its Contract Personnel with un-hosted access to areas within the BT estate; the non BT authorised signatory and Contract Personnel must adhere to the guidance document "Access to BT Sites and Buildings by non BT Organisations" in Annex 4. Additionally the non BT authorised signatory and Contract Personnel shall have as minimum L2 pre-employment checks.

## 9. Physical Security - Supplier Premises

**Compliance to clauses in Section 9 is required if Supplier is providing Supplies from a non BT premises and includes all Contract Personnel, Subcontractors, Supplier's employees, subcontractors and agents.**

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 be by an Authorised Supplier provided 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, for their sole purpose to access the applicable premises or keypad security access with processes to control Authorisation, dissemination and regular Code/ ad-hoc Code change.

9.2 Supplier shall ensure that access to sites, buildings or internal areas where Supplies are carried out, or BT Information is stored or processed, must be authorised and must adhere to security processes and procedures including sub-Contractors with physical access to these areas (e.g. environmental control maintenance, Alarm companies).

9.3 If requested by BT business or BT project owner Supplier shall ensure that Relevant Contract Personnel are segregated in a secure manner from all other supplier personnel.

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 regularly, and re-authorisation of access rights to these areas must be carried out annually as a minimum.

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:-
i) Where CCTV video evidence has to be retained for an incident or criminal investigation.
ii) Where specified as a necessary requirement to adhere to legislation.

All CCTV video tapes used for recording camera images 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.
All CCTV video/digital video recorders must be discreetly located to prevent unauthorised access and the possibility of 'casual' viewing of any associated CCTV screens.

9.6 The local area surrounding Supplier's facilities used for the Products and/or Services, as applicable, shall be inspected for risks and threats on a regular basis by Supplier.

9.7 Power and telecommunication cabling 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:
i) Business critical carriageway, cable shielding, manholes or footway boxes carrying business critical cables must be protected.
ii) 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.
iii) Computer communications links and communications equipment within computer installations must be physically and environmentally protected.
iv) Radio and satellite communications links and communications equipment must be appropriately protected.

9.8 Manned security services are deemed necessary to complement the electronic and physical security measure at supplier locations under the following circumstances:

- Location is of operational importance
- BT Information processed can impact Brand and be reputation impacting
- High volume of BT information processed (e.g. Business process outsource)
- Customer contractual requirements
- Site specific Risk/Threat
- Supplier is in possession of BT information that has a high level of sensitivity.

9.9 To protect BT Equipment (such as Servers or BT Switches) on supplier 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.

9.10 Prevention and detection measures will be employed to prevent installation failure caused by interruption of essential services or other environmental influences.

- Fire,
- Gas,
- Flood
- Power failure

Alarms should be installed and connected back to a permanently manned position to enable detection of the following:

- Fire,
- Gas,
- Power failure,
- Failure of the Uninterrupted Power Supply (UPS),
- Failure of air conditioning/humidity temperature control

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

9.12 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.

9.13 Ensure that physical access to areas that have Access to BT Information is solely with smart or proximity cards (or equivalent security systems) and Supplier conducts regular internal audit to ensure compliance with these provisions.

9.14 Supplier shall ensure that photography and/or the image capture of any BT Information or BT customer Information is prohibited. Under exceptional circumstances where there may be business requirements to capture such images, temporary exemption to this clause must be obtained in writing from BT Security Contact using annex 3.

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

## 10. Provision of Hosting Environment

**Compliance to the clauses in Section 10 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"):
(a) 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
(b) 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
(c) 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
(d) provide BT with a floor plan of allocated space in the secure area of the Supplier Site; and
(e) 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
(f) implement a secure key management process at the Supplier Site; and
(g) inspect the local area surrounding the Supplier Site for risks and threats on a regular basis; and
(h) document and maintain operating procedures (in the language of the country originating the BT Work) to discharge the security requirements detailed within this paragraph 12 and on request provide BT with access to such documentation.

10.2 BT shall provide the Supplier with:

(a) a record of BT's and/or BT's customer's physical assets held at the Supplier Site; and
(b) details of BT's employees, subcontractors and agents that need access to the Supplier Site (on an on-going basis).

## 11. Development of Supplies

**Compliance to these clauses in Section 11 is required if Supplier is dealing with development of Supplies for use by BT and/or BT Customers. (This includes "components off the shelf", Configurations of software and manufacturing components for the Supplies)**

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

(i) 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
(ii) minimizes the opportunity of unauthorised individuals (e.g. hackers) from gaining access to BT Systems and BT Information, BT Networks or BT Services, and
(iii) minimizes the risk of misuse of BT Systems and BT Information, BT Networks or BT 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 ensure that 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 to Industry best practice

11.4 ensure that development and test environments do not contain live data and are segregated from the live environment. BT provided test data must be deleted after a period determined by the BT data owner.

11.5 The Supplier warrants that all reasonable efforts have been made to ensure the Software and/or hardware (and Documentation provided in electronic format) is free from, including but not limited to all forms of

(i) "electronic possession" and "logic bombs";
(ii) "viruses" and "worms" that could have been detected by using the latest (at the date of despatch) commercially available virus detection software; and
(ii) "spyware", "adware" and other malware.

(which expressions shall have meanings as they are generally understood within the computing industry); Supplier warrants upon and after its acceptance, the Software and/or hardware will perform in accordance with the Functional Specification during the Warranty Period; and Supplier shall employ only good quality materials, techniques and Security Requirements in performing the Contract and at all times apply the Security Requirements of care, skill and diligence required of good computing practice and secure coding methodologies.

11.6 The Supplier shall work with BT to ensure compliance with security requirements to the appropriate security framework(s) at the Supplier's cost; from time to time this may require Supplies to be security tested accordingly.

11.7 Any security weaknesses in the Supplies identified by BT or the Supplier shall be remedied at the Supplier's cost within such timescales as BT shall reasonably require.

## 12. Access to Information

**Applicable if specified in the Requirements.**

12.1 Within 14 days of BT's written request and at BT's option either:

(a) the Parties shall, bearing their own respective expenses, execute and deliver to the other an access to information agreement in the form of the Access to Information Agreement as set out in Appendix 3; or

(b) the Supplier shall at the Supplier's own expense, enter into an escrow deposit arrangement substantially in the form of the agreement set out at Appendix 21 in respect of all Information and documentation in relation to Supplies (including, without limitation, in respect of Software, all source code, linkage data, software listings, full technical data, programmer's notes, all information and documentation relating to the Software which is necessary for maintaining, modifying and correcting the Software and providing all levels of support for the Software) ("the Escrow Information") and deposit in escrow with NCC Escrow International Limited (the "Escrow Agent") an up-to-date copy of the Escrow Information. The Supplier shall ensure that such Escrow Information shall enable BT and/or any competent third parties on BT's behalf to:

(i) complete any outstanding obligations of the Supplier under the Contract, including, without limitation, obligations that would have existed (including the requirement to fulfil any orders that BT would have otherwise placed under the Contract) had the Contract not been terminated by BT (other than pursuant to paragraph 4 of the Condition headed "Termination") before the expiry of its natural term (which shall include any extended term under any option by BT to extend the initial term) ; and

(ii) readily to understand the Escrow Information, maintain (including to upgrade), modify, enhance and correct the Escrow Information and the Supplies.

12.2 The Supplier warrants that the Escrow Information deposited either with BT or with the Escrow Agent, as the case may be, is and will be maintained as sufficient to allow a reasonably skilled programmer or analyst to maintain or enhance the Software without the help of any other person or reference, and the Supplier further undertakes to keep the Escrow Information fully up-to-date throughout the Term.

12.3 On occurrence of any event permitting BT or the Escrow Agent, as the case may be to use and/or release the Escrow Information, the Supplier shall immediately provide at its cost and expense, to BT for a reasonable period, such advice, support, assistance, data, information, access to key personnel of the Supplier or its licensor of the Software for the purpose of understanding, maintaining (including upgrading), enhancing, modifying and correcting any of the Escrow Information and/or the Software.

12.4 Without affecting any other rights it may have, BT shall automatically have the non-exclusive, perpetual, irrevocable, worldwide right, free of charge, to use the Escrow Information, after its release, in order to maintain and support the Supplies and with the non-exclusive, perpetual, irrevocable, worldwide and free of any payments right to use, copy, maintain (including to upgrade), modify, adapt, enhance and correct the Supplies and

any modified, adapted, enhanced and/or corrected Supplies, and to license such Supplies to third parties (subject to the limitations of any licences to the Supplier), together with the right to authorise third parties to do any of the aforesaid on BT's behalf.

12.5 This Condition shall survive the expiry or termination of the Contract.

12.6 If required for the purposes of ensuring compliance in relation to security matters, the BT Network Security Contact (and/or his nominees, who shall all be employees of BT) shall have similar rights (mutatis mutandis) if requested as part of the Supplies, of Familiarisation and Validation (as defined in the Access to Information Agreement) in respect of Source Material (as defined in the Access to Information Agreement).

## 13. Access to BT Systems

**Compliance to the clauses in Section 13 is required if Suppler Contract Personnel need to access BT Systems in order to provide Supplies.**

13.1 BT may allow at is sole discretion, to the extent that BT determines, access solely for the provision of Supplies, whilst supplier is Authorised to have access.

13.2 In relation to access, Supplier shall (and, where relevant, shall ensure that all Contract Personnel shall):

a) 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.

b) On reasonable request provide to BT reports as BT shall require concerning Contract Personnel Authorised to access BT Systems.

c) Inter domain linking to BT Systems is not permissible unless specifically approved and authorised by BT Security Contact using annex 3.

d) 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.

e) Use reasonable endeavours to ensure that personal files which contain information, data or media with no relevance to the Supplies are not stored on BT servers, BT Provided laptops and desktops, BT centralised storage facilities or BT Systems.

13.3 If BT has provided Supplier with access to the Internet/Intranet, Supplier shall, and shall ensure that the Contract Personnel, access the Internet/Intranet appropriately to enable it to provide the Supplies, as applicable. It is Supplier's responsibility to ensure that the following guidance on internet and email abuse is communicated to the Relevant Contract Personnel as a minimum annually.

Must not access material which could be considered to be: -

a. Offensive, sexual, sexist, racist, politically offensive;
b. An act that may bring BT or individuals into disrepute;
c. Running a private business;
d. An infringement of copyright;

e. Internet telephony or messaging, such as Skype
f. Bypassing or tunnelling through BT's firewall or other security mechanisms;
g. Must not contribute to sites or post online statements that could be reasonably attributed as the views of BT.
h. Unacceptable or dangerous sites should be blocked from the user.

13.4 Supplier shall notify BT immediately if any Relevant Contract Personnel no longer require access rights to BT Systems or change role for any reason whatsoever from the Agreement thus enabling BT to disable or modify the access rights to BT Systems.

## 14. Access to BT Information on Supplier Systems

**Compliance to the clauses in Section 14 is required if BT Information is being stored or Processed on Supplier Systems.**

14.1 If Contract Personnel are granted Access to Supplier Systems related to Supplier's delivery of Products and/or Services to BT, Supplier shall:

a) ensure each individual has a unique user identification and password (that conforms to industry standard best practice) known only to such individual for his/her sole use as part of the secure login process.
b) allow Access to Supplier owned Systems that hold or access BT Information or BT Systems only to the minimum extent required to enable the Contract Personnel to perform their duties under the Agreement.
c) maintain formal procedures to control the allocation, review and revocation and/or termination of access rights.
d) ensure that the allocation and use of enhanced privileges and access to sensitive tools and facilities in Supplier Systems are controlled and limited to only those users who have a business need. System consoles must be accessed and operated in a secure environment which is commensurate with the assets they are used to manage. Appropriate physical security must be put in place to ensure that unauthorised access cannot occur.
e) ensure that the allocation of user passwords to Supplier owned Systems that hold or access BT Information is controlled through a formal auditable management process.
f) conduct regular reviews of user access rights.
g) ensure that physical access to computing equipment having access or storing BT Information is solely with smart or proximity cards (or equivalent security systems) and Supplier conducts regular internal audit to ensure compliance with these provisions.
h) demonstrate that users follow security best practice in the management of their passwords.
i) implement a password management system which provides a secure and effective interactive facility that ensures quality passwords.
j) ensure that user sessions are terminated after a defined period of inactivity.
k) Ensure that audit logs are generated to record user activity and security-relevant events and are securely managed. Logs shall be retained for a reasonable period to facilitate any investigation with nil ability on the part of Supplier to allow any un-authorised access or amendment to the audit logs.
l) ensure that monitoring of audit and event logs and analysis reports for anomalous behaviour and/or attempted un-authorised access are performed by Supplier's personnel independent of those users being monitored.

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, IPS etc.

14.3 maintain controls to detect and protect against malicious software and ensure that appropriate user awareness procedures are implemented.

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

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

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

14.7 ensure code reviews and penetration testing on all in-house produced software used to process BT information is performed by a team independent to the developers.

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 Changes to individual Supplier Systems which hold and process BT Information and/or which are used to provide the Products and/or Services to BT, must be controlled and subject to formal change control procedures.

14.10 All systems must have their internal clocks synchronised to a trusted source.

## 15. Supplier Hosting BT Information

**Compliance to the clauses in Section 15 is required where Supplier is externally hosting BT Information classified as In Confidence or above 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 requirements in Annex 5.

## 16. Network Security

**Compliance to the clauses in Section 16 is required where 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 and such security:

(a) meet all legal and regulatory requirements; and
(b) 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
(c) uses its best endeavours to reduce the risk of misuse of the BT Networks and/or 21CN, which could potentially cause loss of revenue or service, by those individuals who are authorised to access it; and
(d) uses its best endeavours to detect any security breaches that do occur enabling quick rectification of any problems that result and identification of the individuals who obtained access and determination of how they obtained it; and
(e) Minimise the risk of misconfiguration of BT Networks e.g. may be achieved 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 supplied components, and should not assume that the supplied components are operated in a secure environment.

16.3 The Supplier shall provide to the BT Network 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 Network Security Contact (or his nominees) and to attend such meetings as the BT Network Security Contact shall from time to time reasonably require.

16.5 The Supplier shall provide the BT Network Security Contact with a schedule (updated as necessary from time) of all active components comprised in the Supplies 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. The Supplier shall provide BT with timely information on vulnerabilities, and comply with such reasonable requirements in relation to vulnerabilities as may be notified by the BT Network Security Contact from time to time, at the Supplier's cost. The Supplier shall inform BT of any vulnerabilities in sufficient time to allow mitigating controls to be instated ahead of the Supplier releasing the vulnerabilities publicly.

16.7 The Supplier shall permit the BT Network Security Contact and his nominees from time to time full and unrestricted access to any premises where the Supplies are developed, manufactured, or fabricated to perform security compliance testing and/or assessment, and the Supplier shall co-operate (and shall ensure that all relevant Contract Personnel co-operate) in such 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:

(a) 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;
(b) 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;
(c) when it is transmitted, adequate security is applied to it by encrypting with Secure Email, PGP or WinZip 9; and
(d) 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 Network 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:

(a) the Supplier knows; or
(b) the BT Network 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 Network 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 Network monitoring tools that can view application information must not be used.

16.13 IPv6 functionality included in operating systems must be disabled on hosts (end user devices, servers) connecting to BT network domains should be disabled where not required.

16.14 Supplier shall comply and shall ensure that Supplies comply with BT policies if provided and Security Requirements, any non-compliance must be agreed at contract signature or under change control.

16.15 The Supplier shall ensure that all Contract Personnel have pre-employment checks appropriate to level of Access
http://www.selling2bt.bt.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 Network 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.

## 17. Supplier Network Security

**Compliance to the clauses in Section 17 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, implement security measures across their networks, such that it safeguards the confidentiality, availability and integrity of BT Information. The measures shall:-

(a) meet all legal and regulatory requirements; and
(b) use its best endeavours to prevent unauthorised individuals (e.g. hackers) from gaining access to the Network and
(c) use its best endeavours to reduce the risk of misuse of the Networks which could potentially cause loss of revenue or service, by those individuals who are authorised to access it; and
(d) use its best endeavours to detect any security breaches that do occur enabling quick rectification of any problems that result and identification of the individuals who obtained access and determination of how they obtained it.

## 18. Cloud Security

**Compliance to the clauses in Section 18 is also required when the Supplier is providing BT with Cloud related Services. Definition of Cloud can be found in NIST Publication http://csrc.nist.gov/publications/nistpubs/800-145/SP800-143.pdf)**

18.1 Suppliers shall provide appropriate evidence that the Cloud Services being provided meet the control requirements of the Cloud Security Alliance Cloud Controls Matrix (CCM) to the latest issued version available at https://cloudsecurityalliance.org in addition to compliance with Annex 5 of these security requirements.

18.2 BT Information involved in electronic commerce passing over public networks shall be protected in accordance with Annex 1 whilst in-transit and at rest (Including Back-ups) from fraudulent activity; and unauthorised disclosure, access and modification.

18.3 Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer requirements.

18.4 Supplier shall permit penetration testing and/or access to existing supplier penetration test reports relevant to the Supplies being provided, the scope and timing of the testing to be mutually agreed with BT.

18.5 Supplier shall, implement agreed security measures across all supplied components, such that it safe guards 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 Services.

## Glossary

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**" – 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 Buildings for the provision of services (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 business or BT project owner; "**authorisation**" shall be construed accordingly. Access level provided will be relevant and limited to that required to provide the Supplies.]

"**BT Items**" - all items provided by BT to Supplier and all items held by Supplier which belong to BT. (e.g. keys to cabinets, laptops tokens, pass cards, plans, process documents.)

"**BT Network Security Contact**" - Information Assurance Professional from BT Security, contacted by completing and submitting request form in Annex 3, or such other person whose identity and contact details may be notified to the Supplier's Commercial Contact from time to time.

"**BT Physical Assets**" - all Physical Assets held by Supplier which belong to BT. (e.g. Routers, switches, servers or documentation)

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

"**BT Security Contact**" – Information Assurance Professional from BT Security, contacted by completing and submitting request form in Annex 3.

"**BT Security Policy**" means relevant BT's network security policy as supplied by BT.

"**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 or on behalf of BT, BT Group plc or any entity of BT Group plc; or such other systems that may be hosted on BT Premises (including iSupplier (as "iSupplier" is defined in the Agreement Section headed "Payment and Invoicing") used in the context of "Access" (as defined above).

"**CCTV**" - means close circuit television

"**Commencement Date**" – as defined in the contract.

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

"**Information**" – means information whether in tangible or any other form, including, without limitation, specifications, reports, data, notes, documentation, drawings, software, policies, procedures, processes, standards, 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.

"**ISO 27001**" - an international security management system standard by the International Organisation for Standardization and the International Electro technical Commission.

"**Order(s**)" - an order by BT to Supplier for Supplies placed in accordance with the Contract.

"**Network Security**" - means the security of the interconnecting communication paths and nodes that logically connect end user technologies together and associated management systems.
"**Personal Data**" - shall have the meanings ascribed to them in Directive 95/46/EC or any subsequent legislation in relation thereto ("The Directive").
"**Process," "Processed" or "Processing**" means any operation, or set of operations, which is performed upon BT Information , whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, return or destruction
"**Sensitive Information**" - any BT Information classified or marked as "In Confidence" or above, including Personal Data.
"**Subcontractor**"- as defined in 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 Single point of contact for Security related issues.
"**Supplies**" - all components, materials, plant, tools, test equipment, documentation, firmware, Software, spares and parts and things to be provided to BT pursuant to the Contract together with all Information and Work the Contract requires be supplied to or performed for BT.
"**Transfer" or "Transferred**" means
(a) 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
(b) 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.