

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

Table of Contents

1. Introduction and Scope	2
2. Security of Information for Limited Access	2
3. General Information Security	3
4. Contract Personnel Security.....	6
5. Audit & Security Review	7
6. Investigation.....	8
7. Generic Security Requirements & Policy	8
8. Physical Security - BT Premises.....	9
9. Physical Security - Supplier Premises	10
10. Provision of Hosting Environment	12
11. Development of Supplies	13
12. Access to Information	14
13. Access to BT Systems.....	15
14. Access to BT Information on Supplier Systems	16
15. Supplier Hosting BT Information	18
16. Network Security	18
17. Supplier Network Security.....	21
18. Cloud Security	22
19. Contact Centre	22
Glossary	23

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

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 -7, are mandatory for all other types of work.

For the 3rd level depending on the scope of work one or more requirements in sections 8-19 may be applicable, your BT Procurement representative will be able to advise.

Some of the requirements may reference guidance or standards as listed below which provides additional information. :

- BT's Data Classification & Handling Requirements
- Security of Information Training
- Access to BT Sites and Buildings by non BT Organisations
- External Hosting Security requirements
- Contact Centre 3rd Party standard
- Third Party-Industry Guidance Standards on 'Secure Coding'

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 a 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).

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

Sections 3 - 7 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 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 at (Risk.compliance@bt.com) of the individual(s) Contact details and any change to them. Details should include:-
Responsibility, role and group email address and/or telephone number

3.2 At commencement of the Contract the Supplier shall notify the BT Security Contact at risk.compliance@bt.com of the geographical locations where the main services are delivered, relevant Contract Personnel are located and/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 at risk.compliance@bt.com, so BT may re-assess any risk to BT or BT Customer Information.

3.3 If the Supplier is permitted to subcontract 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.

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. The Supplier shall handle or use BT Information in a manner that is consistent with the requirements in 3rd Party Information Classification and Handling Specification <http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm> and in accordance with all applicable laws and regulations.

3.5 The Supplier shall notify BT Security contact at risk.compliance@bt.com, should the Supplier be subject to a merger, acquisition, or material changes in ownership or control as soon as reasonably practicable, so we may re-assess any risk to BT and BT or BT Customer information.

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 these Security Requirements to ensure they are complying with all applicable Security Requirements.

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

3.7 The 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 The 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".

The Supplier shall inform BT Security Contact at risk.compliance@bt.com or nominated BT 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 it comes to the Supplier's attention. Relevant security incidents include 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 data, information or systems). These incidents may include, but are not limited to, the following:

- loss of service, equipment or facilities;
- corruption, damage or misuse of BT Physical Assets and/or, BT Items;
- 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.

Without unreasonable delay, the Supplier shall take appropriate, timely corrective action to mitigate any risks and effects related to the incident and reduce the severity and duration of the incident.

The Supplier agrees to provide the following information when notifying BT of a relevant security incident that affects the provision of data and/or any part of the Services provided to BT: -

- Date and time
- Location
- Type of incident
- Impact
- Classification of information impacted
- Status
- Outcome (resolution recommendations or actions taken)

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

3.9 The 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 a security risk review on relevant parts of the service being provided by the Supplier (which may include subcontractors relevant to the service) to identify additional risks to BT. BT may then require additional countermeasures to address any risks. Any costs associated with the implementation of required countermeasures will be agreed by the Supplier and BT. Examples of when a risk review may be required include:

- a serious Security Incident affecting the service
- a change in Geographical location of the service
- a change to the scope of work

3.11 The 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 5 below.

3.12 The 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, the Supplier should refer to the most current version of the 3rd Party Information Classification and Handling Specification available at

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

3.13 The Supplier shall have a documented procedure for the identification and treatment of threats against BT. As a minimum, the procedure should describe:

- the events that constitute a threat
- the method by which these should be communicated to those responsible for dealing with the threat
- the agreed notification path into BT (if not part of a generic procedure)
- a record of threats identified and remedial action taken

3.14 The 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. If remote access via public networks for support purposes is utilised, the connections will be encrypted using encryption conforming to at least the standards documented in the most current version of the 3rd Party Information Classification and Handling Specification available at

<http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm>. The remote user must be strongly authenticated using two-factor authentication.

3.15 On termination or the expiration of the Contract, the Supplier shall, and shall procure that any Contract Personnel and Subcontractors, securely destroy in accordance with the most current version of the 3rd Party Information Classification and Handling Specification available at

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

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

3.16 BT information may be retained for as long as necessary to perform the service 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, within the constraints of laws and regulations applicable to the Supplier.

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 implementing appropriate security measures. Such measures may include but are not limited to covering the following:

- availability of appropriate personnel;
- environmental services availability;
- availability of servers;
- networks and communications availability;
- data and software availability;
- A backup plan is in place, which is tested as a minimum annually.
- fall-back arrangements if this is an agreed requirement
- data and software availability; and
- back-up copies of information/data and software where applicable shall be taken and tested regularly in accordance with an agreed backup policy to ensure restoration of data and or software without alteration

Where the Supplier is responsible for changes to a production environment, any planned change activity must have a full back out plan to restore the environment to a known working baseline.

4. Contract Personnel Security

4.1 Relevant Contract Personnel shall not be granted Access until they have completed BT's Security of Information Training Accessible via <https://workingwithbt.extra.bt.com>. (Supplier personnel provided with BT UIN's will access the training via BT's learning system as directed on receipt of UIN) 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 at <https://workingwithbt.extra.bt.com>. 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 The Supplier shall deal with breaches of security policies and procedures, through formal processes including disciplinary action as appropriate, which may include removal of the individual from BT project. Additionally the Supplier should ensure they have relevant processes in place to ensure any Contract Personnel who have been removed from a BT project as a result of a security breach is not subsequently able to undertake work for BT.

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

4.4 The 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 at risk.compliance@bt.com.

4.5 When Contract Personnel are no longer assigned to the Supplies, the 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 the most current version of the 3rd Party Information Classification and Handling Specification available at <http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm>. 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.

4.7 The Supplier shall have policies and processes in place to ensure Contract Personnel must not use social media to publish, post, or send online statements that

- could be reasonably attributed as the views of BT
- release any BT Information that is confidential
- commentary, content, or images that are defamatory to BT, and might cause harm to BTs brand and reputation.

5. Audit & Security Review

5.1 To assess the Supplier's compliance of these Security Requirements BT or its appointed representatives reserve the right to conduct security audits (subject to the Supplier maintaining the confidentiality of information relating to its other clients) from time to time, on any or all aspects of the Supplier's policies, processes and system(s) by a document based security review or at Supplier's and any relevant Subcontractor's site(s) that are materially involved in the provision of the Supplies or performing the Contract.

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 an onsite audit.

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 by BT or such period as agreed between the parties.

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

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

shall, at its own expense, undertake 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 breach by the Supplier or any Subcontractor of the provisions of these Security Requirements, which impact BT Systems and/or BT Information, BT shall inform the Supplier Security Contact. The Supplier agrees, at its own cost:

- to take action immediately to investigate the security breach and to identify, prevent and make reasonable efforts to mitigate the effects of any such security breach,
- to carry out any recovery or other action necessary to remedy the security breach.

In the event of a serious breach 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, by providing access and assistance as necessary and appropriate 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.

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 The Supplier's system, associated services, processes and physical location shall be ISO27001 certified or shall comply with the Security Requirements of ISO27001 certification or have security policies aligned to ISO27001 and/or working towards ISO27001 within a timeframe agreed with BT.

Where the Supplier is certified to ISO/IEC 27001:2013 the certificate must be provided by a certification body accredited by an IAF affiliated accreditation body and subject to regular independent audit by the same.

7.2 The Supplier must abide by applicable policies and standards at <http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm>. Additionally if provided BT may update from time to time, security related 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 The 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.

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

7.4 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 scheme available at <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>. This is a government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks.

For clause sections 8-19, the description for each section specifies what sort of Supplies the clauses apply to.

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.

Where Contract Personnel have been issued with permanent BT access cards Supplier must notify BT promptly and in any event within 5 working days when such Contract Personnel no longer requires access to BT premises, e.g. they leave or move roles.

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 at risk.compliance@bt.com 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. In any event Supplier must ensure that no equipment personally owned by its employees, (including contractors, temporary employees and agency workers) is used to store, access or process any BT data.

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 "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.

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

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 as a minimum monthly Code and ad-hoc Code changes.

9.2 Supplier shall ensure that access to non BT premises where Supplies are carried out, or BT Information is stored or processed, must be authorised and must adhere to security processes and procedures for control of employees, visitors and other persons external to Supplier, including sub-Contractors with physical access to these areas (e.g. environmental control maintenance, Alarm companies, cleaners).

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. Additionally Supplier must ensure that the systems and infrastructure used to deliver the Service 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 as a minimum monthly and 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, or 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 Services. BT must be informed before any substantial works that could compromise the security of BT's information and data are undertaken

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.

PUBLIC DOCUMENT

BT Supplier Security Requirements V2.0

All CCTV video/digital video recorders must be securely located to prevent modification or deletion and the possibility of 'casual' viewing of any associated CCTV screens.

Guidance on CCTV can be found here

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

9.6 The area of supplier premises to the boundary used for the Products and/or Services, as applicable, shall be inspected for risks and threats as a minimum monthly by Supplier. Supplier must have considered and implemented appropriate measures to ensure physical security with respect to the following:

- awareness of local threats including, but not limited to, potential threats from local industry and proximity of stored hazardous materials; and
- natural disasters, including risks from threats including, but not confined to flooding, landslip or extreme weather.

9.7 Power and telecommunication cabling within Supplier premises boundary 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:

- Business critical carriageway, cable shielding, manholes or footway boxes carrying business critical cables must be protected.
- 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.
- Computer communications links and communications equipment within computer installations must be physically and environmentally protected.
- Radio and satellite communications links and communications equipment must be appropriately protected.

9.8 BT may request that 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 Supplier must have implemented appropriate measures to ensure physical security with respect to the following:

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

- fire prevention measures including but not limited to alarms, detection and suppression equipment;
- climatic conditions: Consideration given to temperature, humidity and static electricity, management, monitoring, response to extreme conditions (such as automatic shutdown, alarms);
- control equipment including, but not limited to air conditioning and water detection;
- building: location of water tanks, pipes etc.
- auditable access – where appropriate access to systems by personnel must be auditable; and
- supplier employees and /or contractors / third parties not normally associated with the management of BT's systems must be supervised.

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 with smart or proximity cards (or equivalent security systems) and Supplier conducts as a minimum monthly 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 at risk.compliance@bt.com.

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

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

(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 record of BT's and/or BT's customer's physical assets held at the Supplier Site; and
- 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:

- 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
- minimizes the opportunity of unauthorised individuals (e.g. hackers) from gaining access to BT Systems and BT Information, BT Networks or BT Services, and
- 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 Systems and processes used for test and development activities must be segregated from production systems. A change control process must be used for the promotion of code to the production environment. BT provided test data must be deleted after a period determined by the BT data owner, no live/production data can be used in development or test environments.

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

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

all vulnerabilities, viruses and malware. All critical security vulnerabilities found in security testing and classified as medium risk or above must be fixed prior to going live. 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 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.

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

11.8 Software or applications 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 EE within the audit framework described in clause 5.1:

- security review of the business requirements;
- security review of the design;
- security review of the source code – automatic and/or manual;
- 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. 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

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

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 Supplier Contract Personnel need to access BT Systems in order to provide Supplies.

13.1 BT may allow at its 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

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

- 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 at risk.compliance@bt.com.
- 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 The Supplier with access to BT systems 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 clause 5.1:

The Supplier with access to BT systems must notify BT promptly and in any event within 5 working days when an employee, including contractors, temporary employees and agency workers, no longer requires access to BT systems, E.g. employees leave or move roles.

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 demonstrate accountability (including, but not limited to use of unique user accounts, password management and non-repudiation through audit of logs); and

Supplier must ensure an automated audit trail is implemented for all system components to reconstruct the following:

- individual accesses to data
- actions taken by individuals with root or administrative privileges
- access to all audit trails
- invalid logical access attempts
- use of identification and authentication mechanisms
- initialization of the audit logs

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

- creation and deletion of system level objects

For each auditable event, the audit trail must capture at a minimum, the below listed entries for all system components:

- user identification and authorisation
- type of Event
- date and time of event
- success or failure indication
- origin of event
- identity or name of the affected data, system component or resources

14.2 Supplier shall maintain systems which detect and record any attempted damage, modification or un-authorized 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 Supplier must ensure 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:

- Online credentials for BT customers must contain the following as a minimum:
 - o user ID
 - o online password
 - o 3 authentication questions & answers to support account access
 - o an alternate method of contact for authentication purposes
- The BT customer must be able to choose a unique User ID for their online credentials
- The BT customer's online password must not contain the User ID.

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

- 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; decimal number (0-9), capital case letter (A-Z), lower case letter (a- z), non-alpha numeric
- To change an online password the BT customer must provide their current password followed by double entry of the new password.
- When a BT Customer User-ID or password is forgotten, the system must generate an email to the registered email address containing the User-ID or password request link after successful entry on the online form of the following:
 - o MSISDN or Landline number
 - o online password
 - o BT Customer User ID
- The password reset request link must have a limited duration of validity of at most 30 minutes before it expires and a new reset of online password request has to be made.
- On successful password reset, the BT Customer User must be forced to change to a new password.
- 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.
- 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 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 3rd Party External Data Hosting Requirements available at <http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm>.

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

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

- (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:

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

- (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.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.

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

16.17 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 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)

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:-

- meet all legal and regulatory requirements; and
- use its best endeavours to prevent unauthorised individuals (e.g. hackers) from gaining access to the Network and
- 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
- 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.

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

- use of effective "defence in depth" principles (<https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525>);
- controls must be in place that prevent any purposeful attack;
- use of firewalls, routers, switches;
- secure communications between devices and management stations; and
- secure communications between devices as appropriate; including the encryption of all non-console administrator access.
- strong architectural design, which is tiered and zoned and effective with robust identity management, operating system configuration must be appropriately hardened and documented;
- services, applications and ports that will not be used must be disabled where practical;
- guest accounts must be removed or disabled;
- the most recent security patches must be installed on the system as soon as practical following testing, any exception must be communicated to BT where they will be risk assessed. BT reserves the right to obligate Supplier to install patches following risk assessment;
- trust relationships between servers must be avoided;
- use of best practice security principle of "least privilege" to perform a function; and
- appropriate measures must be in place to handle Denial of Service attacks;
- appropriate measures must be in place for intrusion detection and/or protection;
- monitoring all applicable vendors and other relevant information sources for vulnerability alerts;
- where appropriate, measures must be in place for file integrity monitoring to detect any additions, modifications or deletions of critical system files or data
- all default and vendor supplied passwords must be changed before the system goes live

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://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.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 BT's External Hosting Security requirements available at <http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm>.

18.2 BT Information involved in electronic commerce passing over public networks shall be protected in accordance with 3rd Party Information Classification and Handling Specification available at <http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm> 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.

19. Contact Centre

Compliance to the clauses in Section 19 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>.

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

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” – BT Group, EE and subsidiaries.

“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 at Risk.compliance@bt.com, 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 at Risk.compliance@bt.com

“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

“Contract Personnel” **“Relevant Contract Personnel”** - as defined in the contract.

“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.

“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”).

PUBLIC DOCUMENT
BT Supplier Security Requirements V2.0

“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.