Contents

1. Introduction

1.1 This document sets out BT's Security Requirements and applies to all 3rd party's working for or on behalf of BT Group, including Openreach, EE and PlusNet, here on referred to as 'BT' for the rest of the document.

1.2 These Security Requirements are in addition to and without prejudice to any other obligations of the 3rd party in the Contract.

1.3 All standards referred to in this document can be found at the following location. 3rd Party Standards

2. Limited Access Requirements

2.1 Without prejudice to any obligations of confidentiality it may have, where 3rd Party Personnel have Access to BT Information, the 3rd party must:

2.2 Ensure BT Information is not disclosed to or Accessed by 3rd Party Personnel unless necessary for the provision of the Service; and

2.3 Put in place all systems and processes both technical and organisational as are required to protect BT Information (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or Access to BT Information in accordance with Good Industry Security Practices.

3. General Information Security

3.1 On reasonable request the 3rd party shall make available to BT copies of security certifications and statement of compliance relevant to the Service in order to illustrate evidence of compliance with these Security Requirements.

3.2 Should there be a significant change to technology or industry security standards; or there are any material changes to the Services or how they are provided, BT may issue a Contract amendment during the term, if there is a need for a change to the applicable Security Requirements. The 3rd party shall comply with the agreed Contract amendment within a reasonable time considering the nature of change and the risk to BT.

3.3 The 3rd party must as a minimum annually or when there are any material changes to the Services or how they are provided, review these Security Requirements and associated standards to ensure they are still compliant to all applicable security controls.

3.4 If the 3rd party subcontracts obligations under the Contract, then the 3rd party shall ensure all Contracts with relevant Subcontractors and their Subcontractors, include written terms requiring the Subcontractor to comply with the applicable parts of either these Security Requirements or to equivalent 3rd party security requirements.

3.5 BT Information may be retained for as long as necessary to perform the Contract, after which it should be retained no longer than a maximum of two years, unless a different retention period has been agreed between BT and 3rd party or is required by any applicable laws.

3.6 If the Services are in direct support of a UK Government Contract, the 3rd party must comply with the most current version of the Cyber Essentials Plus.

3.7 The 3rd party must ensure the BT Information is handled as per the controls in the following standards:

- 3rd Party Information Classification and Data Handling Standard V4.0
- Our Standard on 3rd Party Controls V1.1 – Sections

  Section 1 Roles & Responsibilities.

  Section 2 Governance.

  Section 3 Incident Management.

  Section 4 Change Management.

  Section 5 Cyber Risk and Threat Management

  Section 6 Identity Management and Access Control.

  Section 10 Data Classification and Protection.

  Section 12 Data Leakage Prevention.

  Section 13 PCI-DSS (if in scope of the Service).

  Section 19 Vulnerability Management.

  Section 22 Continuous Logging and Monitoring.

4. 3rd Party Personnel Security

4.1 The 3rd party shall ensure that all 3rd Party Personnel have confidentiality agreements in place before any 3rd Party Personnel start working in BT buildings or on BT Systems or have Access to BT Information. These confidentiality agreements must be retained by 3rd party and evidence be made available for audit by BT.

4.2 The 3rd party shall deal with breaches of 3rd party and applicable BT security controls and standards, through formal processes including disciplinary action which may include removal of the individual from:

4.2.1 having Access to BT Systems or BT Information; or

4.2.2 carrying out work connected with the provision of the Service.

In addition, the 3rd party should ensure they have relevant processes in place to ensure any 3rd Party Personnel who have been so removed are not subsequently given Access to BT Systems, BT Information or allowed to work in connection with the provision of the Service.

4.3 The 3rd party shall, to the extent permissible by the law, maintain a confidential facility, to be used by the 3rd Party Personnel to anonymously report if they are instructed to act in a manner inconsistent or in violation of these Security Requirements. Relevant reports to be notified to BT.

- When 3rd Party Personnel are no longer assigned to the Service, at BT's option, any BT physical assets or BT Information in the possession of 3rd Party Personnel should be either: handed back to the relevant BT operational team;
- destroyed in accordance with 3rd Party Information Classification and Data Handling Standard V4.0

4.4 The 3rd party must ensure there are appropriate processes in place regarding 3rd Party Personnel to discharge the controls in the following standards:

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 15 Social Media

section 23 Training and Awareness

5. Audit & Security Review

5.1 Without prejudice to any other right of audit that BT may have, in order to assess the 3rd party's compliance to these Security Requirements and associated standards, the 3rd party 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 3rd party prior to a routine onsite audit.

The scope of the audit will be to review any or all aspects of the 3rd party's policies, processes and system(s) (subject to the 3rd party protecting the confidentiality of any information not related to the provision of the Service to BT), that are relevant to the Service being provided.

5.2 The 3rd party will work with BT to implement agreed recommendations and carry out any corrective actions identified as 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 at the 3rd party's expense.

5.3 Should BT need to conduct an independent audit of the 3rd party and the 3rd party is found to be non-compliant with the principles and practices of ISO/IEC 27001:2013 then 3rd party shall, undertake at its own expense those actions required in order to achieve the necessary compliance and shall reimburse in full any costs incurred by BT in obtaining such audit.

6. Right of Inspection

6.1 The 3rd party must give BT the right of inspection as per:

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 24 Right of Inspection.

7. Security Certifications

7.1 The 3rd Party Systems, Service, associated Services, processes and physical locations must be compliant with and shall continuously comply with the ISO/IEC 27001:2013 standard (or certification(s) that demonstrate equivalent controls, supported by an independent auditor report) and any amended or future version of the standard issued. This compliance must be assured either by:

7.1.1 certification of the 3rd party's ISMS by a UKAS or an international equivalent approved certification body where the scope and statement of applicability has been validated by BT; or

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

7.2 The 3rd party must submit a valid certificate at the start of the Contract and on future re-certifications.

7.3 Should the scope of the certificate or statement of applicability be changed at any time, the 3rd party must submit these changes for re-validation using the change control procedure (or, in the absence of a change control procedure, through the variation process). The 3rd party must inform BT within 2 working days of any major non-conformance identified by the certification body or the 3rd party.

8. Physical Security – BT Premises

8.1 Where the 3rd party is working within BT premises, the controls in the following standard will apply:

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 25. Physical Security – BT Premises

9. Physical Security – 3rd party Premises

9.1 Where 3rd party premises are used to provide the Service, the controls in the following standard will apply.

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 9. Physical Security in 3rd Party Premises **excluding** controls 9.10 and 9.11 for Provision of hosting environment for BT equipment.

10. Provision of Hosting Environment for BT Equipment

10.1 Where 3rd party premises are used to provide an equipment hosting environment, the controls in the following standard will apply.

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 9. Physical Security in 3rd Party Premises - controls 9.10 and 9.11 for Provision of hosting environment for BT equipment.

11. Secure software Development

11.1 Where 3rd party is providing software or systems, the controls in the following standard will apply.

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 17. (17.1 and 17.2) Secure Software Development

12. ESCROW

12.1 Where ESCROW is required to protect all parties, the controls in the following standard will apply.

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 17. (17.3 only) Secure Software Development

13. Access to BT Systems

13.1 Where 3rd Party Systems or 3rd Party Personnel require Access/connection to BT Systems, the controls in the following standard will apply.

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 8. Access to BT Systems

14. 3rd Party Systems holding BT Information

14.1 Where 3rd Party Systems are used which will hold BT Information, the controls in the following standards will apply:

3rd Party 3rd Party Information Classification and Data Handling Standard V4.0

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 7 Information Asset Management.

Section 11. Cryptography.

Section 16 System Configuration.

Section 18 Anti-Malware Protection**.**

Section 21. Denial of Service Mitigations.

15. 3rd party Hosting BT Information

15.1 Where 3rd party is hosting BT's information the premises must hold a valid ISO/IEC 27001 certificate for security management (or certification(s) that demonstrate equivalent controls, supported by an independent auditor report).

15.2 The controls in the following standards will apply:

- 3rd Party 3rd Party Information Classification and Data Handling Standard V4.0
- Our Standard on 3rd Party Controls V1.1 – Sections

Section 7 Information Asset Management.

Section 11. Cryptography.

Section 16 System Configuration.

Section 18 Anti-Malware Protection**.**

Section 21. Denial of Service Mitigations.

16. Network Security – BT's own Network

16.1 Where 3rd party will be installing equipment, configuring, maintaining, repairing or monitoring BT's own network the controls in the following standard will apply:

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 26. Network Security – BT's own Network.

17. 3rd party Network Security

17.1 Where 3rd party's own network will be used to Access BT Information or to provide the Service the controls in the following standard will apply:

- Our Standard on 3rd Party Controls V1.1 – Sections

Section 16 System Configuration.

Section 20 Network Integrity

18. Cloud Security

18.1 Where 3rd party will be providing BT with cloud Services the controls in the following standard will apply:

- Our Standard on 3rd Party Controls V1.1 – Sections
  Section 14. Cloud / Online Computing.

19. Contact Centre

19.1 Where 3rd party will be providing BT with contact centre Services the controls in the following standard will apply:

- Contact Centre 3rd Party Standard V1.0

20. Information classified as OFFICIAL or higher by HMG

20.1 Where the Supplier is required to access, store, process or transmit information classified as HMG OFFICIAL or higher Supplier to conduct a Personnel Security Risk Assessment on all roles identified in Official Sensitive Declaration para 2 in line with the requirements set out in the document CPNI National Security Clearance - A guide (4th Edition - June 2013 or later).

20.2 The additional Security Requirements set out in Annex 1 to these Security Requirements will apply to each 3rd party that will store, process or transmit information classified as 'Official Sensitive' in line with Her Majesty's Government Security Classifications Scheme as updated from time to time.

20.3 The 3rd Party will ensure that the systems and infrastructure used to deliver the Services are contained within a dedicated logical network. This network must consist only of the systems dedicated to delivery of a secure customer data processing facility.

21. Defined Terms and Interpretation

21.1 Unless otherwise defined below, words and expressions used in these Security Requirements will have the same meaning as in the Contract:

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

a. by interconnection with BT Systems;

b. provided in paper or non-electronic format;

c. BT Information on Supplier Systems; or

d. by mobile media

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

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

"**BT Systems**" means the Services and Service components, products, networks, servers, processes, paper-based system or IT systems (in whole or part) owned and/or operated by BT or such other systems that may be hosted on BT premises.

"**Contract**" means the Contract entered into by the Parties for the supply of goods, software or Services which references these Security Requirements.

"**Cyber Essentials Plus**" means UK Government backed scheme to help organisations protect themselves against common cyber-attacks.

"**Escrow**" means the source code deposit agreement entered into in accordance with the Contract, to use, copy, maintain and modify such source code for the business purposes of BT (including the right to compile such source code).

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

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

"**Official Sensitive Declaration**" means the written declaration to be provided by the Supplier relating to roles identified by the Supplier as having Access to information classified as "Official Sensitive" or having elevated privileges to infrastructure that stores, processes or transmits information classified as "Official Sensitive", a template of which is set out in Annex 1.

"**Security Requirements**" means this document as updated from time to time.

"**Subcontractor**" means a Subcontractor of the Supplier which performs or is involved in the provision of the Supplies or which employs or engages persons engaged in the provision of the Supplies.

"**3rd Party Personnel**" means any persons engaged by the Supplier or its Subcontractors in the performance of the Supplier's obligations under the Contract.

"**Service**" means any and all of the "**Goods**", "**Software**" or "**Services**" as defined in the Contract.

"**3rd Party Systems**" means any Supplier owned computer, application or network systems used for accessing, storing or processing BT Information or involved in the provision of the Supplies.

Interpretation

21.2 Any words following the terms "including", "include", "in particular", "for example" or any similar expression will be construed as illustrative and will not limit the sense of the words, description, definition, phrase or term preceding those terms.

21.3 Any time a Party's right or obligation is expressed as one that they "**may**" exercise or perform, the option to exercise or perform that right or obligation will be in that Party's sole discretion.

21.4 Where any hyperlink ("**URL**") is referenced, such reference will be to such online resource Accessible via that URL or such other replacement URL as notified to the applicable Party from time to time.

Version	Description	Author	Date
4.0	New	Karen Tanner	02/02/20
4.1	Additional clause for HMG clause set 20	Karen Tanner	20/02/20

ANNEX 1 – Additional Security Requirements

Where the 3rd Party is required to Access, store, process or transmit 'HMG Official Sensitive' information, the 3rd Party will comply with these Security Requirements and additionally the requirements set out in this Annex 1 and provide BT with the completed Official Sensitive Declaration prior to Contract signature. In all cases, the highest-Level control will supersede requirements documented elsewhere in these Security Requirements for the Services and systems set out in the Official Sensitive Declaration.

1. EMPLOYEES

1.1. All roles identified by the 3rd Party as having Access to information classified as "Official Sensitive" or having elevated privileges to infrastructure that stores, processes or transmits information classified as "Official Sensitive" will be documented in the Official Sensitive Declaration.

1.2. 3rd Party Personnel employed in roles identified in the Official Sensitive Declaration:

1.2.1. must be subject to pre-employment screening to Baseline Personnel Security Standard (BPSS) standard as a minimum;

1.2.2. must sign an Official Secrets Act declaration; and

1.2.3. that are unable to obtain the required security clearances must be prevented from accessing information or systems.

2. SECURITY TRAINING

2.1. The 3rd Party will mandate security training upon hire and at least annually, covering information handling requirements for information classified as "Official" or "Official Sensitive" in line with the requirements of Her Majesty's Government Security Classifications Scheme as detailed in BT's protecting HMG information guidance for 3rd parties

2.2. The 3rd Party will update job descriptions for the roles documented in the Official Sensitive Declaration to mandate participation in training described in paragraph 2.1 above. The 3rd Party will maintain a record of training which must be made available to BT upon request.

3. ACCESS CONTROL

3.1. When employees leave or move roles, their Access rights must be revoked from relevant 3rd Party Systems within one (1) Business Day.

3.2. Where the 3rd Party's employees, including Contractors, temporary employees and agency workers, have elevated privileges to the BT infrastructure, the 3rd Party must notify BT in writing within 1 Business Day from when an employee no longer requires Access to BT Systems (e.g. employees leave or move roles).

3.3. Where the 3rd Party's employees, including Contractors, temporary employees and agency workers, are issued with permanent Access cards to BT premises, the 3rd Party must notify BT in writing within 1 Business Day when an employee no longer requires Access to BT premises (e.g. employees leave or move roles).

4. VALUATION AND CLASSIFICATION OF ASSETS

4.1. The 3rd Party will implement additional information handling procedures to meet handling requirements for "Official" or "Official Sensitive" information in line with the

requirements of Her Majesty's Government Security Classifications Scheme as updated from time to time

5. INCIDENT RESPONSE AND REPORTING – SERVICE LEVEL AGREEMENTS

5.1. The 3rd Party will be advised on specific Service level agreements to support the incident response process. These may supersede any previous agreement outlined in these Security Requirements.

6. AUDIT, TESTING AND MONITORING

6.1. The 3rd Party will implement 24/7 security monitoring where specified by BT

6.2. The 3rd Party's infrastructure subject to 24/7 security monitoring will be documented in the Official Sensitive Declaration.

7. BUSINESS CONTINUITY AND DISASTER RECOVERY

7.1. The 3rd Party will produce a business continuity and disaster recovery plan in accordance with BS ISO 22301 within 30 days of Contract signature.

8. LOCATION

8.1. Unless specified otherwise by BT, the Service must be physically located within the physical boundaries of the UK or, if applicable, the EEA.

ANNEX 1, EXHIBIT 1 – OFFICIAL SENSITIVE DECLARATION TEMPLATE

1. Systems/Services in Scope

Please list the systems and Services being provided in support of the HMG customer.

System	Service

2. 3rd Party roles requiring a security clearance level.

Role	Required Security Clearance Level
* *e.g. DBA*	*SC*

3. Vulnerability Management

System	Type of vulnerability Assessment	Frequency

4. Audit, Testing and Monitoring

Systems to be monitored 24/7 as advised by BT