Public

PROTECTING BT

Our Standard on 3rd Party Controls

Version: 1.1 **Owner:** Mark Tilston

This standard sets the basic security controls for our 3rd Parties.

It's published and communicated to all applicable parties and will be owned and reviewed by the 'Subject Matter Expert's' at least annually, to ensure it continues to meet the requirements of interested parties and our business objectives as described in BT's ISMS.

It applies to all 3rd party's working for or on behalf of BT Group, including Openreach, EE and PlusNet.

To keep it simple we'll just say 'BT' for the rest of the document.

Where an activity is to be carried out by a BT Stakeholder this is highlighted in Grey.

Introduction

BT is committed to providing a secure environment that our customers and employees can trust. Our aim is to protect all our information and systems against accidental or malicious destruction, damage, modification or disclosure. This is supported by ensuring we implement the right 3rd Party control measures to protect the confidentiality, integrity and availability of our information and systems.

Who does this apply to?

This standard applies to any 3rd party who works for, or, on behalf of BT, who comes into contact with BT information or data, that is accessed, processed, stored, or distributed by the 3rd party. We may change this standard from time to time, subject to any agreed internal consultation processes.

Definition of terms:

Term	Explanation
must	This word, or the terms 'REQUIRED' or 'SHALL', means that the definition is an absolute requirement
must not	This phrase, or the phrase 'SHALL not', means that the definition is an absolute prohibition
may	This word, or the adjective 'OPTIONAL', means that an item is truly optional
should	This word, or the adjective 'RECOMMENDED', means that there be a valid reason in certain situations to ignore a specific item, but the implications will be fully understood and carefully assessed before choosing a different option.
should not	This phrase, or the phrase "NOT RECOMMENDED" means every effort will be made to meet the requirements of a control, but it might not always be possible to avoid the action being described in all cases. Where a control can't be complied with the implications will be assessed and fully understood.

Scope

This document describes at a high level the minimum-security controls required to manage security within BT's 3rd Party supply chain.

BT Personnel can find supporting standards as well as the baselines, process documents and guidelines describing the implementation of the controls which must read in conjunction with this standard on the security website.

BT Stakeholders who require an exemption for a 3rd party to this standard must be make a request through the Exemptions Process

What's included in this document?

1. Roles & Responsibilities.

Every 3rd Party must be aware and understand the requirements of this standard and are responsible for making sure that all individuals who are involved in providing a service to BT are familiar and comply with the relevant requirements of this standard.

BT Stakeholders have a responsibility to oversee compliance to this standard and work with their 3rd Party to improve compliance and implement mitigations when gaps are identified.

BT managers are responsible for making sure their people are familiar and comply with the requirements of this standard and associated policies and standards.

2. Governance.

2.1. The 3rd Party must have an established and consistent industry standard security framework for information and cyber security governance which covers the following components:

- Appropriate Information and Cyber Security policies and procedures which are approved and communicated
- An information security strategy
- Relevant legal and regulatory requirements regarding Information and Cyber Security (including privacy) which are understood and managed
- Governance and risk management processes which address information and cyber security risks

2.2. The 3rd Party must ensure that appropriate roles and responsibilities for Information and Cyber Security defined and implemented which includes the following:

- A full-time Chief Information Security Officer (or equivalent) who is sufficiently senior and has responsibility for information security programme
- A high-level working group, committee or equivalent body which coordinates information security activity across the 3rd Party which is chaired by a suitably senior member of staff and meets on a regular basis
- A specialist information security function with suitable and defined roles and responsibilities

2.3. The 3rd Party must ensure that there is individual accountability for information and systems by ensuring that there is appropriate ownership of critical business environments, information and systems and that this is assigned to capable individuals

2.4. The 3rd Party must ensure that BT is notified (in writing) as soon as they are legally able to do so if the 3rd Party is subject to a merger, acquisition or any other change of ownership

3. Incident Management.

3.1. The 3rd Party must have an established and consistent incident management framework to ensure that incidents are appropriately managed, contained and mitigated and covers the following components:

- Ensuring that personnel know their roles and order of operations when a response is needed
- Ensuring incidents reported consistent with established criteria
- Ensuring that the impact of the incident is understood
- Ensuring that forensics are performed where necessary either internally or by a specialist function
- Ensuring that lessons learned from incidents are incorporated into best practice.
- Ensuring information related to an incident impacting BT is treated as “Confidential”.

3.2. The 3rd Party 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. 3rd Party shall notify BT Stakeholder of the individual(s) Contact details and any change to them. Details should include: -
Name, responsibility, role and group email address and/or telephone number

3.3. The 3rd Party will inform the BT Stakeholder, within a reasonable timeframe upon becoming aware of any incident that impacts the service to BT or BT information, and in any event, no later than twelve (12) hours from the time the Incident comes to 3rd Party's attention.

3.4. The 3rd Party without unreasonable delay, will take appropriate and timely corrective action to mitigate any risks and effects related to the incident in order to reduce the severity and duration of the incident.

3.5. The 3rd party will provide a report to the BT Stakeholder in respect of any incident that impacts the service to BT or BT information, it should include as a minimum:

- date and time
- location
- type of incident
- impact
- classification of information impacted (See 3rd Party Information Classification and Data Handling Standard)
- status
- outcome (including the resolution recommendations or actions taken).

3.6. If a 4th party will be used to provide the service, where they will hold or process BT Information, the 3rd party must obtain agreement from the BT Stakeholder what information can be shared. The 3rd party must ensure they have a contractual relationship with the 4th party and must ensure the 4th party has an industry standard security framework.

4. Change Management.

4.1. The 3rd Party must ensure that all IT changes are approved, logged and tested, including backing out of failed changes, prior to implementation to prevent service disruption or security breaches and that there is a process for undertaking emergency updates in a controlled manner.

4.2. The 3rd Party must ensure that changes are reflected in Production and DR environments.

4.3. The 3rd Party must notify BT immediately of any material changes to the service (such as but not limited to) changes to its access method through the firewalls, including the provision of network address translation.

4.4. The 3rd Party must ensure that maintenance and repair of organisational assets is performed and logged, with approved and controlled tools.

4.5. The 3rd Party must ensure that remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorized access.

5. Cyber Risk and Threat Management

5.1. The 3rd Party must ensure that there is an ongoing Cyber Security risk and threat assessment framework to ensure that the Cyber Security risk profile to the organisation's operations, assets, premises and individuals is understood and managed by:

- Assessing asset vulnerabilities
- Identifying both internal and external threats
- Sensitivity of information / data in scope
- Assessing potential business impacts
- Threats, vulnerabilities, likelihoods, and impacts are used to determine risk?
- Ensuring that the Cyber risk and threat management framework is agreed at a suitable level in the organisation.

5.2. The 3rd Party must ensure that all risks and threats identified as part of the Cyber Security Risk and threat assessment are prioritised and action taken accordingly to mitigate the risks in a suitable timescale.

5.3. The 3rd Party must notify BT Stakeholder if they are unable to remediate or reduce any material areas of risk that could impact the service being provided.

6. Identity Management and Access Control

6.1 The 3rd Party must have an established and consistent framework to ensure that identities and credentials are managed securely by authorised personnel:

- Only granting, re-enabling, changing and disabling of access rights based on documented and authorised approvals.
- Ensuring that dormant accounts are disabled.
- Disabling accounts of personnel who are no longer in employment.
- Periodic reviews of access are in place to ensure that access is fit for purpose.
- User accounts have access recertified on at least an annual basis and privileged accounts have access recertified quarterly.

6.2 The 3rd Party must ensure that remote access is managed so that only approved individuals can connect remotely to the 3rd Party's systems and that connections are secure and prevent data leakage and appropriate access control is in place such as multi-factor authentication.

Two factor authentication should be achieved with a User ID, Password and one of the following methods:

- A one-time password generator; that requires a user specific PIN/password to view the one-time password.
- A smart card with an ISO 7816-compliant chip and associated card reader and software. Contactless smart cards are not permitted.
- Certificate based authentication issued in accordance with your Infosec certificate policy.

For avoidance of doubt if privileged access for support is provided via remote access, then this must be via a secure connection and use 2 factor authentication.

6.3 The 3rd Party must ensure that access permissions and authorisations for all systems (including tools, applications, databases, operating systems, hardware etc.) are managed incorporating the principles of least privilege and separation of duties.

6.4 The 3rd Party must ensure that each transaction can be tied back to one unique sole identifiable individual and if there are any shared credentials that there are appropriate compensating controls (including break glass procedures).

6.5 The 3rd Party must ensure that all authentication is managed commensurate with the risk of the transaction, i.e. appropriate password length and complexity, frequency of changes of passwords, multi-factor authentication, secure management of password credentials or other controls.

6.6 Appropriate controls must be in place to handle failed authentications, including screen notifications, logging of failure and user lockout.

6.7 Processes and controls must be in place to manage and authorise guest and service accounts.

7. Information Asset Management

7.1. The 3rd Party must have an information asset inventory (which if applicable should include any BT equipment hosted in 3rd party premises) and ensure that there is at least one test annually to validate that the Information asset inventory is current, complete and accurate.

7.2. The 3rd Party must ensure that the information asset inventory has the following components inventoried or catalogued:

- Physical Devices and Systems, Software Platforms and Applications, External Information Systems
- Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value
- Organisational and Communication Data Flows including external / 3rd party flows
- Manual processes that handle BT or BT Customer data.

8. Access to BT Systems

8.1 The 3rd Party shall adhere to all relevant instructions provided to them with regards to access and use of BT Systems.

8.2 3rd Party is responsible for advising BT with 24 hours when a 3rd party individual no longer requires access.

8.3 The 3rd party shall ensure user identification, passwords, PINs, tokens, and conferencing access are for individual 3rd Party personnel and not shared. Details must be stored securely and separately from the device that is used to access. If a password is known by another person, it must be changed immediately.

System to System connectivity

8.4 Inter domain linking to BT Systems is not permissible unless specifically approved and authorised by BT.

8.5 The 3rd party must use all reasonable endeavors to ensure no viruses or malicious codes (as the expressions are generally understood in the computing industry) are introduced to BT Systems.

8.6 Where there is connectivity between the 3rd Party and BT systems the connectivity will be via secure links with data protected by encryption conforming to the controls in **Section 11 Cryptography**.

8.7 The 3rd Party will ensure that the systems and infrastructure used 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.

9. Physical Security in 3rd Party Premises

9.1 The 3rd Party must have a physical access process that covers access methods and authorisation to 3rd Party premises (sites, buildings or internal areas) where services are provided, or where BT Information is stored or processed. Access method should include 1 or more of the following:

- An authorised 3rd Party identification card with a photographic image displayed on the card that is a clear and be a true likeness of the individual.
- An authorised electronic access card to access the applicable areas of the premises.
- Keypad security access, which must have processes for: authorisation, the dissemination of code changes (which must occur monthly, as a minimum); and ad-hoc code changes.
- Biometric recognition

9.2 The 3rd Party must have processes and procedures for the control and monitoring of visitors and other external persons, including 3rd Party 's with physical access to secure areas or for the purpose of environmental control maintenance, alarm maintenance and cleaners.

9.3 Secure areas in 3rd Party premises used to provide the service (e.g. network communications rooms), shall be segregated from general access areas and protected by appropriate entry controls to ensure that only authorised individuals are allowed access. Access made to these areas must be audited regularly and an assessment of re-authorisation of access rights to these areas must be carried out annually as a minimum.

9.4 The 3rd Party shall have CCTV security systems in locations where BT information is stored or handled.

9.5 CCTV recordings must be retained for a minimum of 20 days. This period may however be extended in the following situations:

- Where CCTV video evidence must be retained for an incident or criminal investigation; or
- Where specified as a necessary requirement to adhere to legislation

9.6 All CCTV recordings and recorders must be securely located to prevent modification, deletion or the 'casual' viewing of any associated CCTV screens and access to the recordings must be controlled and restricted to authorised individuals only.

9.7 The 3rd Party must have implemented appropriate measures to ensure physical security with respect to the following

- Fire prevention measures including but not limited to alarms, detection and suppression equipment.
- Climatic conditions, with consideration given to temperature, humidity and static electricity and the associated management, monitoring and response to extreme conditions (such as automatic shutdown, alarms).
- Control equipment including, but not limited to air conditioning and water detection.
- Prevention of water damage, location of water tanks, pipes etc. within the premises.

9.8 The 3rd Party must ensure that physical access to areas that are hosting BT Information is with smart or proximity cards (or equivalent or better security systems) and 3rd Party must conduct monthly checks to ensure only relevant individuals are provided with this access.

9.9 The 3rd Party must ensure that photography and/or the image capture of any BT Information is prohibited. Where there is a business need to capture such images, confirmation must be obtained in writing from the BT Stakeholder.

Provision of hosting environment for BT equipment.

9.10 The 3rd Party must, where the 3rd Party is providing a secure access area on their premises for hosting BT or BT Customer equipment:

- Provide BT with a floor plan of allocated space in the secure area of the premises.
- Ensure that BT and BT customer cabinets at the premises are kept locked and only accessed by authorised BT personnel, BT approved representatives and relevant 3rd Party personnel.
- Implement a secure key management process.

9.11 BT shall provide the 3rd Party with:

- A record of BT and/or BT customer's physical assets held at the 3rd Party premises.
- Details of BT's employees, subcontractors and agents that need access to the 3rd Party premises (on an on-going basis).

10.Data Classification and Protection.

10.1 The 3rd Party must have an established and consistent information classification and handling framework / scheme (aligned to Good Industry Practice / BT requirements) which contains the following components:

- Information handling guidelines
- Information is protected in line with its assigned level of classification
- Ensuring that all staff aware that BT information shall not be used for any purpose other than that for which it was provided.
- BT's information should be handled as per 3rd Party 3rd Party Information Classification and Data Handling Standard.

11. Cryptography.

11.1 The 3rd Party must ensure that where the level of risk requires encryption, that such data is appropriately encrypted (in transit and at rest) and where cryptographic keys are used that they are designed and implemented to meet the security requirements specified in the NIST FIPS 140-2 Standard at level 2 or above.

11.2 Cryptographic keys must meet or exceed the following minimum lengths:

- Symmetric keys (e.g. AES) must have a key length of at least 256 bits.
- Asymmetric keys (e.g. RSA) must have a key length of at least 2048 bits.
- Elliptic Curve keys must have a key length of at least 224 bits.

11.3 If NIST announces a crypto algorithm is no longer secure, it must not be used for new deployments. Existing deployments must review the continued use of deprecated crypto algorithms and deliver a migration plan to move away from deprecated crypto algorithms to something more secure.

11.4 For symmetric encryption the following algorithms are not allowed; 3DES-168 (unless mandated by an international standard), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed and ARIA.

11.5 Salted hashes must be used to protect data in storage i.e. passwords. Hashing may also be used to anonymise data before processing, for example MSISDNs or payment. The following hashing algorithms are not allowed MD2, MD4, MD5 and SHA-1.

11.6 Key Management - Creation and taking into use

- Session keys and nonces must be created using a secure pseudorandom number generator. This must be seeded with at least as many bits of entropy or the unexpectedness of a message, as the number of effective bits of security provided by the algorithm that will use the key.
- Taking a shorter key of 64bits and combining in a non-cryptographic way, with the same key of 64bits to get 128 bits is forbidden.
- All bits of the key must be taken into use by the algorithm
- Padding or other bits used by algorithm shall not count towards key length

11.7 Key Management – Randomness

- A robust source of random data must be used when producing session keys for use in the symmetric parts of hybrid cryptography, or, for producing salts or initialisation vectors.
- Pseudo-random number generators (PRNG) may be used, but to be considered secure, a PRNG must not enable an attacker to:
  - Guess the future output of the generator, given knowledge of previous output
  - Calculate the previous states of the generator, given knowledge of its current state
  - Distinguish the output of the PRNG from true randomness. (Use of rand() is not allowed.

11.8 Key Management - Key exchange

- Session keys that are generated for use with a symmetric algorithm must be exchanged using a secure key exchange protocol

11.9 Key Management - Key Storage

- Where keys are used to protect data at rest, the data encryption key (DEK) must be protected using a key encryption key (KEK) which must be stored on a separate server, or, stored within a Trusted Platform Module (TPM).
- If the KEK is stored on a separate server it must be protected in transit to the server hosting the data.

11.10 Key Management - Key Rotation (regeneration)

- It must be possible to regenerate the key according industry best practice on key lifetimes.
- It must be possible to re-encrypt the data to be protected with the regenerated key.
- It must be possible to perform ad-hoc regeneration of key and re-encryption of data if there is a suspected compromise of the original encryption key.
- For AES GCM, the probability that the authenticated encryption function ever will be invoked with the same IV and the same key on two (or more) distinct sets of input data shall be no greater than 232

11.11 Key Management - Hardware security modules (HSMs)

- Cryptographic keys must be loaded onto an HSM using smart cards.
- Smart cards must require a PIN to allow access.
- The PINs must be chosen in accordance with the access control policy.
- The PINs and smart cards must be stored in a safe that has been reviewed by your Infosec team.
- It must not be possible to extract cryptographic keys from an HSM.
- HSMs must destroy the cryptographic keys stored in them if an attempt is made to open the case.
- For HSMs that contain highly sensitive keys, the PINs and smart cards used to protect them must be configured and stored only by technology security staff members.
- Where the HSM will be used to protect highly sensitive data, a minimum quorum of 2 smart cards and their associated PINs must be required to make changes to the HSM. Members of the quorum must be vetted at the enhanced screening level.

11.12 Digital certificates

- Certificates must have the Certificate Revocation List Distribution Point (CDP) attribute set.
- Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) must be used for determining certificate status.
- Certificate owners must track the validity and expiry of the certificates owned to ensure that expected expiry events do not cause system failure.
- Certificate consumers (clients) must track the validity and expiry of certificates used to ensure that expected expiry events do not cause system failure.
- Certificate lifetime must be selected appropriate to the purpose of the certificate.
- Certificate lifetime must be established before issue.
- Use of Standard identity (client, server) 1024 not allowed

11.13 Data in transit

- Encryption of data in transit is typically achieved using Transport or Payload (Message or Selective Field) encryption. Transport encryption mechanisms include but are not limited to:
- Transport Layer Security (TLS)
- Secure Tunnelling (IPSec)
- Secure Shell (SSH)

- For transport encryption, the symmetric component must be in accordance with section 12.14 of this standard.
- Transport security protocols must be configured to prevent negotiation of weaker algorithms and/or shorter key lengths, when both end points support the stronger option.
- The SSL protocol must not be used as there are several known vulnerabilities directed at this protocol.
- Initialisation Vectors for stream ciphers and AES in CBC mode must not be predictable.
- The IV/nonce in AES GCM must fulfil the following "uniqueness" requirement:
  - Compliance with this requirement is crucial to the security of GCM
  - Transport security protocols must be configured (e.g. use of direction bits) to prevent known plain text attacks from known messages returned e.g. "nothing to report".
  - Mutual identity verification must be performed during the set-up of the transport.
  - For sensitive short length data requiring payload encryption (encryption keys, passwords, payment card information), asymmetric encryption using at least the minimum key lengths and algorithms detailed in in this document.
  - System management data must be encrypted in transit.
  - The following TLS options are not allowed: TLS v1.0, TLS v1.2, v6.0, TLS v6.1 and SSL (any version)
  - The following SSH (SFTP) options are not allowed: SSH v1
  - The following IPSec options are not allowed: IKE Version 1

11.14 Data at rest

- Data at rest includes data stored in files, databases, temporary and swap locations and on any device, including but not limited to PCs, laptops and other portable devices, servers, tape, SANs, USB, CD, DVD, floppy disk and other removable storage solutions.
- Data defined as confidential or above that is stored in non-volatile memory on any device, must be encrypted.
- Payment Card information stored on any device in non-volatile memory must be encrypted.
- Where symmetric key data is stored protected by an asymmetric key, the asymmetric key must provide equivalent strength, measured by bits of security, to the symmetric key itself.
- System documentation must identify data classification and volumes stored by the system.
- Keys used for decryption must not be stored or backed up with the data they decrypt. Software must be fully tested before being deployed to production systems.

12. Data Leakage Prevention.

12.1 The 3rd Party must have an established and consistent framework to ensure that protection against inappropriate data leakage is in place ensuring protection includes (but not limited to) the following vectors:

- Email
- Internet / Web Gateway (including online storage and webmail)
- USB, Optical and other forms of ports / portable storage etc.
- Mobile Computing and BYOD
- Remote Access Services
- file sharing mechanisms and social media

NB. Removable media / portable devices should be disabled by default and only enabled for legitimate business reasons. Any data stored on removable media or portable devices must be encrypted commensurate with risk. Unauthorised devices must not be connected to the network

(either the vendor's corporate network or BT's systems / network) or used to access non-public information. See, 3rd Party Information Classification and Data Handling Standard for more information on handling removable media.

13. PCI DSS

13.1 The 3rd Party must ensure that if the 3rd Party is in scope for Payment Card Data, that the 3rd Party is appropriately compliant with the PCI-DSS.

14.Cloud / Online Computing.

14.1. The 3rd Party must be certified to the latest version of ISO27017 or have an established and consistent framework to ensure that all use of Cloud technology and non-public data stored in the Cloud is approved and subject to appropriate controls equivalent to the latest version of the Cloud Security Alliance, Cloud Controls Matrix (CCM) .

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

14.3. 3rd Party must implement security measures across all aspects of the service being supplied, such that it safeguards the confidentiality, availability, quality and integrity by minimizing the opportunity of unauthorised individuals (e.g. other cloud customers) from gaining access to BT Information and the services utilised by BT.

15. Social Media

15.1. The 3rd Party must have an established and consistent framework on acceptable use of personal and corporate social media including:

- Ensuring personnel do not post anything libelous, obscene or abusive about the organisation, its clients or customers
- Use of organisation or client logos without prior permission
- Exposing of organisation or client non-public information without prior consent
- Posting of opinions about the organisation its clients or customers which could reasonably be construed as official comment of the organisation or its clients
- Must not release any BT Information that is marked as ‘Confidential or ‘Highly Confidential”.

16.System Configuration.

16.1. The 3rd Party must have an established and consistent framework to ensure that systems are appropriately configured (for both 3rd Party systems and systems provided to BT) including the following components:

- Systems, network devices are configured to function in accordance with security principles (e.g. concept of least functionality and no unauthorised software)
- Ensuring that devices have the correct and consistent time
- Systems are free from any malicious software
- Appropriate checks and monitoring are in place to ensure the integrity of the builds / devices are maintained

17. Secure Software Development.

17.1. The 3rd Party must ensure that production and non-production environments are appropriately controlled by ensuring the following components are in place:

- Segregation of production and non-production environments with segregation of duty
- No live data to be used in test unless prior agreement from the data owners and controls commensurate with the production environment
- Segregation of duties between production and non-production development

17.2. The 3rd Party must have an established and consistent Systems Development framework to prevent security vulnerabilities and Cyber Security breaches which contains the following components:

- Systems are developed in line with Secure Development best practice (e.g. OWASP).
- Code is securely stored and subject to Quality Assurance.
- Code is adequately protected from unauthorised modification once testing has been signed off and delivered into production

17.3. Where Escrow is required to protect all parties for either 1st party or 3rd Party Escrow (i.e. for Intellectual Property / Source code etc.) the 3rd Party must have a consistent and established framework which includes the following components:

- Execution of escrow agreement with independent, neutral and reputable Escrow agent
- Delivery and ongoing updates of source code and other materials to the Escrow agent to ensure the required information is up to date
- Secure storage of source code and other materials until release conditions are met
- Appropriate release conditions
- Ongoing updates, appropriate payments and reviews to the escrow agreement.

18. Anti-Malware Protection.

18.1. The 3rd Party must ensure that the most up to date Malware protection is applied to all applicable IT assets to prevent service disruption or security breaches and ensure that appropriate user awareness procedures are implemented.

NB. Anti-malware to include detection for (but not limited to), unauthorised mobile code, viruses, spyware, key logger software, botnets, worms, trojans etc.

19. Vulnerability Management.

19.1. The 3rd Party must have an established and consistent vulnerability management framework which includes the following components:

- Processes policies and procedures
- Defined roles and responsibilities
- Appropriate tools such as Intrusion Detection Systems and vulnerability scanning systems.

19.2. The 3rd Party ’s vulnerability management framework must ensure that the following are routinely monitored to detect potential cyber security events

- Key systems and assets

- Unauthorised connections
- Unauthorised software / applications
- Network activity.

19.3. The 3rd Party ’s vulnerability management framework must ensure that:

- There are processes established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
- Only authorised tools, technologies, users are permitted
- Identified vulnerabilities are mitigated or documented as accepted risks.

19.4. The 3rd Party must ensure that the latest security patches are applied to systems / assets / Networks/applications in a timely manner ensuring that:

- 3rd Party uses patches obtained from: vendors directly for proprietary systems and patches that are either (i) digitally signed or (ii) verified via the use of a vendor hash (MD5 hashes must not be used) for the update package such that the patch can be identified as coming from a reputable support community for open source software.
- 3rd Party tests all patches on systems that accurately represent the configuration of the target production systems before deployment of the patch to production systems and that the correct operation of the patched service is verified after any patching activity.
- monitoring all applicable vendors and other relevant information sources for vulnerability alerts.
- If a system cannot be patched deploy appropriate countermeasures.

19.5. The 3rd Party must ensure that at least on an annual basis, an independent IT security assessment / penetration test is commissioned on the 3rd Party IT infrastructure and applications used to provide services, including Disaster Recovery sites to identify vulnerabilities that could be exploited to breach data / services and to prevent against any security breaches through Cyber Attacks. The 3rd Party must on reasonable request permit BT access to penetration test reports relevant to the services being provided.

19.6. The 3rd Party must ensure that access to diagnostic and management ports as well as diagnostic tools are securely controlled.

19.7. The 3rd Party must ensure that access to audit tools are restricted to relevant supplier personnel and their use is monitored.

19.8. The 3rd Party must ensure that any servers used to provide the service, are not 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.

20.Network Integrity.

20.1. The 3rd Party must ensure that network integrity is established and maintained by ensuring the following components are appropriately controlled:

- External connections to the network are documented, routed through a firewall and verified and approved prior to the connections being established to prevent data security breaches.
- The network is appropriately designed using “defense in depth” principles to ensure Cyber security breaches are minimised by ensuring appropriate controls that prevent any purposeful attack such as “network segmentation” are in place.
- The design and implementation of the network is reviewed at least annually.
- All wireless access to the network is subject to authorisation, authentication, segmentation

and encryption protocols to prevent security breaches.

- Using secure communications between devices and management stations;
- Using secure communications between devices as appropriate; including the encryption of all non-console administrator access;
- Using strong architectural design, which are tiered and zoned with effective identity management and operating system configuration which must be appropriately hardened and documented;
- By the disabling (where practical) of services, applications and ports that will not be used.
- By the disabling or removal of guest accounts.
- By the avoidance of trust relationships between servers;
- Use of the best practice security principle of “least privilege” to perform a function;
- Ensuring appropriate measures are in place for intrusion detection and/or protection;
- Where appropriate, filing integrity monitoring to detect any additions, modifications or deletions of critical system files or data.
- Change all default and vendor supplied passwords before network components go live.

20.2. The 3rd Party Network should meet all legal and regulatory requirements; and

- Use best endeavors to prevent unauthorised individuals (e.g. hackers) from gaining access to the 3rd Party Network(s);
- Use best endeavors to reduce the risk of misuse of the 3rd Party Network (s) by those individuals authorised to access it.
- Use best endeavors to detect any Security Breaches and ensure quick rectification of any breaches, alongside the identification of the individuals who obtained access and determination of how they obtained it.

21.Denial of Service Mitigation.

21.1. The 3rd Party must ensure that key systems are protected against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

22.Security Continuous Logging and Monitoring.

22.1. The 3rd Party must ensure that there is an established and consistent audit and log management framework which ensures that key systems including applications are set to log key events (including those of privileged access and personnel activity) with such logs being retained for a minimum period of 12 months. As a minimum 3rd Party must ensure that the logs (as appropriate) contain the following events:

- Start and stop points of the logged process.
- Changes to the type of logged events as required by the audit trail (for example the start-up parameters and any changes to them).
- System start-up and shut-down.
- Successful logins.
- Failed login attempts (for example wrong user ID or password).
- Creation, modification and deletion to/of user accounts.
- What asset they were accessing (e.g. data),

- Where they accessed the asset (e.g. IP address),
- When (e.g. time-stamp).

22.2. The auditing and log management framework must include the following components:

- Ensuring that logs of key events are reviewed by an independent function on at least a monthly basis to detect for any unauthorised activities and attack targets and methods
- Exceptions are noted are investigated until resolution
- Logs are collected and correlated from multiple sources and sensors and stored securely and are tamper-proof to enable the reconstruction of such events.
- The impact of any events is determined with incident alert thresholds established and acted upon in a timely manner determined by the criticality of the alarm.

23. Training and Awareness.

23.1. The 3rd Party must ensure that all 3rd Party personnel under their control undertake mandatory security of information training, which includes Cyber Security best practice and protection of personal data within one month of joining and refreshed at least on an annual basis including where appropriate:

- Privileged users
- 3rd Party stakeholders (e.g. Sub-contractors, customers, partners)
- Senior executives
- Physical and Cyber Security personnel

23.2. The 3rd Party must ensure that there is a testing component to verify that the user understands the training and awareness.

24.Right of Inspection.

24.1. The 3rd Party must permit BT to undertake an inspection of the control environment where the services are developed, manufactured, or provided to perform security compliance testing and/or assessments on at least an annual basis (or immediately following an incident).

24.2. The 3rd Party is responsible for the costs of remediating any security weaknesses identified by BT within a timescale as agreed by both Parties.

24.3. In the event of a serious incident the 3rd Party shall fully cooperate with BT in any ensuing investigation by BT, a regulatory authority and/or any law enforcement agency by providing access and assistance as necessary and appropriate to investigate the incident. BT may have need to request the 3rd Party quarantine for evaluation any relevant asset belonging to 3rd Party in order to aid the investigation and 3rd Party shall not unreasonably withhold or delay such request.

25. Physical Security – BT Premises.

25.1 All 3rd Party personnel working on BT premises shall be in possession of, and display prominently, a 3rd Party or BT provided identification card which must include a photographic image displayed on the card that is a clear and true likeness of the 3rd Party personnel. BT may also provide 3rd Party personnel with an electronic access card and/or limited duration visitor card which shall be used in accordance with local issuance instructions.

25.2 Where 3rd Party personnel have been issued with an access card by BT the 3rd Party must notify BT promptly and in any event within 5 working days when any 3rd Party personnel no longer require access to BT premises.

25.3 Only approved BT build servers, BT Webtop PCs and Trusted End Devices can directly connect (plug into LAN port or Wireless connection) to BT domains. 3rd Party must not without the prior written authorisation from BT connect any equipment not approved by BT to any BT Domain.

25.4 Physical protection and guidelines for working in BT premises shall be adhered to, and shall include but not be limited to, the escorting of 3rd Party Personnel and the adoption of appropriate working practices within secure areas.

25.5 Where 3rd Party is authorised to provide its 3rd Party personnel with un-hosted access to areas within the BT estate; the 3rd Party authorised signatory and 3rd Party Personnel must adhere to the guidance document Supplier access to BT's sites - Mandatory security guide

Additionally the 3rd Party authorised signatory and 3rd Party Personnel shall have as minimum L2 pre-employment checks

26. Network Security – BT's own Network.

26.1 The 3rd party shall provide to the BT Security Contact the names, addresses (and such other details as BT shall require) of all individual 3rd party personnel who shall from time to time be directly involved in the deployment, maintenance and/or management of the service before they are respectively engaged in such deployment, maintenance and/or management.

26.2 In relation to its UK-based support activities, the 3rd party shall retain a skilled security team comprised of at least one UK national who shall be available for liaison with the BT Security Contact (or his nominees) and the team shall attend such meetings as the BT Security Contact shall from time to time reasonably require.

26.3 The 3rd party shall provide the BT Security Contact with a schedule (updated as necessary from time) of all active components comprised in the Service and/or the Services and their respective sources.

26.4 The 3rd party shall provide details of its individual personnel who will liaise with the BT vulnerability management (CERT) team in relation to discussion around BT and 3rd party-identified vulnerabilities in the Service and/or Services. The 3rd party shall provide BT with timely information on vulnerabilities and comply (at the 3rd party's cost) with such reasonable requirements in relation to vulnerabilities as may be notified by the BT Security Contact from time to time. The 3rd party shall inform BT of any vulnerabilities in enough time to allow mitigating controls to be applied or installed ahead of the 3rd party releasing the vulnerabilities publicly.

26.5 The 3rd party shall ensure that any security-related components comprised in the Service as are identified by or to BT from time to time are, at the 3rd party's cost, externally evaluated to BT's reasonable satisfaction.

26.6 The 3rd party shall promptly, and in any event within 7 Working Days, provide to the BT Security Contact full details of any features and/or functionality in any the Service (or that are planned in the Roadmap for any the Service) that from time to time:

- the 3rd party knows; or

- the BT Security Contact reasonably believes and so informs the 3rd party are designed for, or could be used for, lawful interception or any other interception of telecommunications traffic. Such details shall include all Information that is reasonably necessary to enable the BT Security Contact to fully understand the nature, composition and extent of such features and/or functionality.

26.7 In order to maintain access to BT Networks and/or systems, 3rd party shall notify BT immediately of any changes to its access method through the firewalls, including the provision of network address translation.

26.8 The 3rd party must not use any network monitoring tools that can view application information.

26.9 The 3rd party shall ensure that IPv6 functionality included in operating systems is disabled on hosts (for example end user devices or servers) that connect to the BT Network and domains should be disabled where not required.

26.10 The 3rd party personnel building, developing or supporting BT Networks or Network Assets shall ensure that all 3rd party Personnel have as minimum L2 pre-employment checks. L3 pre-employment checks will be required for roles identified by the BT Security Contact. Where the 3rd party does not have the capability to directly security clear 3rd party Personnel as part of L3 checks then BT will assist in obtaining clearance at the 3rd party's cost.

26.11 3rd party shall maintain hardware and software according to manufacturers' specifications.

26.12 3rd party shall not use removable media (disks, USB drives, etc.) intended for support and maintenance for any other purpose.

27. Glossary.

Term	Definition
2 factor authentication	Sometimes referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.
3rd Party	People who do work for us, but they're not BT employees
AES	Advanced Encryption Standard (AES), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
ASG	Application Support Group
BT Group	BT Group refers to all CFUs & CUs within the BT Group, including but not limited to Openreach, EE and Plusnet - for the purposes of this document they will be referred to as 'BT' unless stated otherwise
BT Stakeholder	The BT employee who has responsibility for the work that has been placed with the 3rd Party.
CCTV	means close circuit television.
DBA	Database Administrator
DC	Data Centre
Defence in Depth	Is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another mechanism steps up immediately to thwart an attack.
DR	Disaster Recovery
GCM	Galois/Counter Mode is a mode of operation for symmetric-key cryptographic block ciphers that has been widely adopted because of its performance

HDD	Hard Disc Drive
HMG	Her Majesty's Government - Covers government bodies in the UK
ISMS	Information Security Management System. Is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.
ISO 27001	Is an industry standard specification for an information security management system (ISMS).
ISO 27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO 7816	Is an international standard related to electronic identification cards with contacts, especially smart cards, managed jointly by the International Organization for Standardisation (ISO) and the International Electrotechnical Commission (IEC).
NAS	a single storage device which operates on data files.
NIST	The National Institute of Standards and Technology is a physical sciences laboratory, and a non-regulatory agency of the United States Department of Commerce.
PCI DSS	Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle branded credit cards from the major card schemes.
Privileged Accounts	A privileged user is someone who has administrative access to critical systems
RSA	(Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission.
SAN	a local network of multiple devices which operate on disk blocks
SSD	Solid State Drive

28.Change history.

Version no	Date	Change made by	Brief details of change
0.1	30/10/17	Mark Tilston	Initial draft for mapping and content update
0.2	10/04/19	Tim Hunt	Transferred to new format
1.0	01/05/19	Ian Morton	Raised to Issue
1.1	01/10/19	Karen Tanner	Additional controls added as part of BT Security Requirements uplift

29.Document sign off

Role	Date
Mark Tilston	06/11/19

30.Compliance

We appreciate most BT employees act professionally and in line with BT's Values but if you behave in a way that's inconsistent with this standard, BT may take disciplinary action depending on local legislation and regulation.

For anyone else, if you behave in a way that's inconsistent with this standard, we may terminate the arrangements we have with you for your services.

31.Useful Links and Information

For BT personnel:

Here is the link where you can review all BT Polices & Standards .

We review all our policy and standard at least annually. To see our review program click here.

To report a 'Security Incident' please email: Security Control Centre

If you need more information or guidance about this standard or any other security policy or standard, contact security.policy@bt.com

For 3rd Parties:

Here is the link where you can see all relevant Standards and other security conditions.

32. Ownership and Confidentiality

This document shouldn't be shared with any other 3rd Party without the written consent of BT. This standard and any associated documentation remains the property of BT and should be returned if requested.

This document is classified as "Internal" however if downloaded by a 3rd Party it should be handled as "Confidential"