Public

PROTECTING BT

3rd Party Information Classification and Data Handling Standard

Standard: 4.0a **Owner:** BT Security

This standard sets the basic security controls for our 3rd Parties who will access, store or process BT Information.

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.

BT

Introduction

BT classifies data and information into categories depending on the harm that could result from loss or unauthorised disclosure. On creation, all data and information is assessed to determine the appropriate classification category.

Data and information must be retained for an adequate period to meet legal, regulatory and business requirements, at the end of which time it is securely disposed of. Any equipment that stores data must also be disposed of at the end of its operational life. Disposal of equipment must be carried out in the most environmentally sensitive manner.

This standard defines the requirements for information classification, labelling, handling/processing, retention and disposal of BT data and information assets.

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.
BT	This term shall mean BT Group, including Openreach, EE and Plusnet. To keep it simple we'll just say 'BT' for the rest of the document.

Scope

This standard applies to all BT data and information in all formats. This includes all paper, electronic documents, multimedia (photos, video, WebEx etc.), verbal (phone conversations/voicemail) and data and information held in systems, applications or equipment that can store, process or transmit data. The scope of this standard covers information classification, labelling, handling/processing, retention and disposal.

What's included in this document?

1. Information Classification Overview.

Not all information that will be held or processed by you as a 3rd party to BT will have the same value or sensitivity. It will be BT's responsibility to classify information in scope of the service you will be providing to ensure that the correct level of protection is applied to information and that information is handled efficiently and securely.

The BT classification scheme has the following four categories:

- Public
- General
- Confidential
- Highly Confidential

If you have not been advised of the classification for the information you are handling, please contact your BT Stakeholder or Procurement Buyer.

2. BT Classification Levels.

Public

Information which has been specifically approved for general publication. There are no special handling requirements associated with information of this classification

Examples include: Details of our products and services, information published on BT external website, press releases, white papers, advertising materials.

General

Information of which unauthorised disclosure, particularly outside BT, would be inappropriate. It is not considered in the interests of BT to release this into the public domain. This information can be limited to specific teams or functions within the business.

NB. When accessed and or stored by a 3rd party the handling classification changes to "Confidential"

Examples include: Employee and business information on the intranet, majority of BT policies, standards, processes and procedures, majority of project related documentation and the majority of minutes for meetings

Confidential

The unauthorised disclosure of this information even within the organisation could cause significant harm to the interests of BT. This information is limited to, and only shared with, authorised individuals to perform a specific business need as part of their job role. Damage could result in financial loss, loss of profitability or opportunity, embarrassment or loss of reputation or lead to a legal or regulatory sanction against BT. Personal information, Payment Card Information or Intellectual Property is classified as 'Confidential'. Confidential information has specific handling requirements which must be adhered to.

Examples include: Personal information about our people, 3rd parties or customers (including related financial payments) such as: Employee Contracts, performance data, CARE surveys, Personal Service Identifier (Service ID, Broadband Identifier, PSTN Identifier). Some project documentation for critical infrastructure or projects, network diagrams, 3rd party supplier contracts. System log data; Sales and marketing data (tariff changes prior to launch, financial performance prior to publication to the markets); Local business plans; Risk data; Call data records and Information that's legally confidential.

Highly Confidential

The disclosure of this information is likely to negatively impact the achievement of key business objectives. This information is exceptionally sensitive in terms of its ability to cause serious damage if leaked. Highly confidential information is limited to a small number of individuals. There must be absolute denial of access to unauthorised persons. The handling requirements are more stringent than those for handling confidential information. This classification is the most restrictive due to the very serious harm that may occur. You may be asked to sign a non-disclosure agreement (NDA) or an 'Insider list', if you handle this information.

Examples include: Computer passwords, a security risk register, certain sensitive personal information such as Payment card information, National Insurance Number, Passport details. Sensitive HR information which may alienate a significant number of employees, strategic business plans, competitive strategy, new strategic products, and new marketing policies, very sensitive competitor, partner or contractor assessments, internet usage, customer account number, audit reports or findings containing details of serious shortcomings/vulnerabilities in BT practices or processes, information which could affect our share price including board minutes, price sensitive information, information relating to mergers and acquisitions, security events, encryption keys, documentation relating to corporate strategy, pre-release business plans, high value projects, and their contract negotiations/terms.

3. Handling and Processing Requirements.

Note: Where not specifically included there are no special handling requirements associated with information with a classification level of 'Public'.

3.1 Handling Spoken and Multimedia.

Reference	What do you want to do with the information	Classification	Handling requirements
HSMS10	I want to post information on social media/networking	Public	You can post to any group e.g. Splash or Yammer. You must not contribute to sites or post online statements that could be reasonably attributed as the views of BT.
		General/Confidential	Not Allowed.
		Highly Confidential	Not Allowed
HSMS20	I want to discuss with or present someone via internal instant messaging e.g. Microsoft Lync	General/Confidential	You can use internal/BT Live Meeting, Webex, Webjoin and Skype for Business. Ensure you have selected and confirmed you have the correct individuals before discussing a specific topic and the following must not be disclosed: · **Any payment card information.** · **Personal Data** · **Bank details.** · **PIN or any other password.**
		Highly Confidential	Not Allowed.
HSM30	I want to discuss with someone via external live chat. e.g. on a vendor support site such as Cisco	Public	Conversations must be restricted to 'public information' that is freely available on our external BT website
		General/Confidential	Only allowed once you have verified the identity of the person/s you are chatting with to have a 'need to know' before you reveal any confidential information of individual/s and the following must not be disclosed: · **Any payment card information.** · **Personal Data** · **Bank details.** · **PIN or any other password.**
		Highly Confidential	Not Allowed.

HSM40	I want to discuss with someone via face to face/phone call	General/Confidential	You must verify the identity of the person you are speaking to has a 'need to know' before you discuss any confidential information (this includes conversations in-store, and call centres) If applicable, an NDA must be in place before starting the conversation. Ensure the conversation cannot be overheard by those with no 'need to know'. You must not leave this information on voicemail systems.
		Highly Confidential	As 'Confidential'. Keep any 'Highly Confidential' information to the absolute minimum.
HSM50	I want to text to all parties (internal & external)	Public	Message content must be restricted to 'public information' that is freely available on our external BT website.
		General/Confidential	Message content is restricted on a 'need to know basis' and the following information must not be disclosed: · **Any payment card information.** · **Bank details.** · **PIN or any other password.** · **Any personal information.**
		Highly Confidential	Not Allowed.

3.2 Handling Paper Documents.

Reference	What do you want to do with the information	Classification	Handling requirements
HPD10	I want to store, copy, print or work on hardcopy information in the office.	General/Confidential	BT Information should not be used in hardcopy form unless specifically part of the scope of work or approved by the BT Stakeholder, then the following applies: You must protect against accidental disclosure. You must clear away when not in use and at close of business and store in an area that's restricted to authorised personnel only e.g. locker, locked drawer or restricted room. Use an access controlled printer, a printer connected to a PC, or a printer in an access controlled room and check you're sending to the right printer. You must use the secure print function to retrieve printed material at the printer unless immediate collection is ensured.
		Highly Confidential	Not Allowed
HPD20	I want to print while in a BT Building	General/Confidential	Check you're sending to the right printer and don't leave documents in the print tray. Use an access-controlled printer, a printer connected to a PC, or a printer in an access controlled room.
		Highly Confidential	As 'General/Confidential'
HPD30	I want to copy or print information which is not our 3rd party premises or at my home (e.g. it's in subcontractor premises, a hotel etc.)	General/Confidential	Not allowed.
		Highly Confidential	Not allowed.

HPD40	I want to carry hardcopy information outside of an BT office, 3rd party Premises or Store	General/Confidential	**You must not remove BT customer and/or payment data from BT offices, 3rd party Premises or stores.** Other types of information must also not be removed unless specifically part of the scope of work or approved by the BT Stakeholder, then the following applies: You must handle with due diligence. You must protect against accidental compromise e.g. (carry in an opaque folder or bag). You must not leave unattended. If lost, you must raise a security incident and notify your BT stakeholder as soon as is possible to do so.
		Highly Confidential	Not Allowed
HPD50	I want to share or send hardcopy information to Internal parties.	General/Confidential	BT Information should not be used in hardcopy form unless specifically part of the scope of work or approved by the BT Stakeholder, then the following applies: You must place document in an internal use envelope or windowless envelope and either deliver by hand or post using your internal post system. Must not be sent to home based Internal parties. Do not indicate the level of classification on the outside envelope. If the information is covered by 'legal privilege' follow your legal privilege guidelines If lost, you must raise a security incident and advise the BT Stakeholder as soon as it is possible to do so.
		Highly Confidential	Not Allowed
HPD60	I want to share or send hardcopy information to external parties	General/Confidential	Not Allowed
		Highly Confidential	Not Allowed

HPD70	I want to send a fax	General/Confidential	You must send header page with a test page, then contact recipient to confirm receipt prior to faxing content. If the information is covered by 'legal privilege' follow your legal privilege guidelines.
		Highly Confidential	Not allowed
HPD80	I want to dispose of hardcopy information	General/Confidential	You must check to make sure that the information is not required to be retained for legal or regulatory reasons. Must be shredded to a minimum of P4 DIN66399 standard using a cross cut shredder (this includes Payment Card information). Never put it in a general waste bin.
		Highly Confidential	You should not be in possession of this classification of Information in hardcopy, however if you are the following applies You must check to make sure that the information is not required to be retained for legal or regulatory reasons. Must be shredded to a minimum of P4 DIN66399 standard using a cross cut shredder (this includes Payment Card information) or may be incinerated in compliance with BS EN15713:2009. Never put it in a general waste bin. **NB. Certain information may require the material to be shredded on site by an external certified 3rd party. If this is the case you must obtain a certificate of destruction from the 3rd party.**

3.3 Handling Electronic Documents.

Reference	What do you want to do with the information	Classification	Handling requirements
HED10	I want to store electronic information on my work provided laptop/PC	All BT Data	Working copies can be kept on your work laptop only if it has full disk encryption e.g. Through a product like Bitlocker. This converts information into unreadable code which can't be deciphered easily by unauthorised people. Completed documents must be securely stored and working copies removed from the laptop.
HED20	I want to store my documents on Document management system e.g. SharePoint or on a network Drive	General/Confidential	Restrict who can edit the site and documents to only those with approval to do so. The document management system / Network drive owner or admin must: - Use permission levels and groups to set up role-based access control. These must be set to no more than the minimum level required for people to do their jobs. - Review the access controls each year. - Document the process for assigning people to roles. - Roles and people assigned must be reviewed at regular intervals, preferably quarterly. **NOTE: document management systems or network drives must not be used to store Payment Card Information**
		Highly Confidential	As 'General/Confidential' and: Documents must be encrypted before uploading to document management system. You should also set a date when access to your document will be revoked.

			NOTE: document management systems or network drives must not be used to store Payment Card Information
HED30	I want to store electronic information in the cloud or with Internet Services (where there is no commercial contract in place to host BT information) such as Google docs, Github, Drop Box, Pastebin, Facebook etc.	All BT data	Not allowed.
HED40	I want to Store electronic on removable media e.g. a memory stick	All BT data	Allowed only if you have an authorised business need to carry BT information outside of the office, but all devices or information must be encrypted. If lost, you must raise a security incident and notify the BT Stakeholder as soon as practicable. **NOTE: removable media must not be used to store Payment Card Information**
HED50	I want to store electronic documents or information on my personal laptop or device.	All BT data	Not allowed.
HED60	I want to send electronic documents to my personal e-mail address	All BT data	Not allowed.
HED70	I want to auto-forward to an external email address	All BT data	Not allowed.

HED80	I want to share or send electronic documents to Internal parties	General/Confidential	You must only share with Internal parties BT General/confidential Information where they have a need to know to perform their job role and: · Make clear the email contains BT General/confidential information. · Use sensitivity settings to mark the email as Confidential · Set the permissions to 'Do not forward' **NOTE: Payment card information should never be held on a PC but if it must be - including sending via email - then it must be encrypted at all times.**
		Highly Confidential	You must only share with internal parties BT highly confidential information where they have a need to know to perform their job role and: · Make clear the email contains BT Highly Confidential information. · Use sensitivity settings to mark the email as Highly Confidential · Set the permissions to 'Do not forward' · Use Secure email to send (If this is not available you must encrypt the information) **NOTE: Payment card information should never be held on a PC but if it must be - including sending via email - then it must be encrypted at all times.**

HED90	I want to share or send electronic documents to an external party	All BT data	You must only share or send to an external party where there is an approved business need or other justification such as an NDA. · You must only share or send to an external party on a need to know basis where there is an approved business, contractual or legislative need and with the approval of the BT Stakeholder. - Ensure any documents and emails show the data classification level. · You must ensure the external party knows the document classification level and is aware of the protection requirements. · You must encrypt the information · You must confirm you're sending to the correct email address. - You will still need to follow the legal privilege guidelines if applicable.
HED91	I want to email a large group of BT employees (100+), (e.g. for employee surveys, training, benefits)	General/Confidential	You must follow our 3rd Party guide on email briefings
		Highly Confidential	Not Allowed
HED100	I want to Internally transfer a BT document or BT information not using email, Skype/Lync for Business or removable media.(e.g. because the file is too large)	All BT data	You can use an internet file transfer facility that is approved for use by your own Security Policy. You must encrypt the document at source before uploading.

HED110	I want to externally transfer a BT document or BT information not using email, Skype/Lync for Business or removable media (e.g. because the file is too large)	General/Confidential	You must only share or send to an external party where there is an approved business need or other justification such as an NDA, which has been approved by the BT Stakeholder · You must only share or send to an external party on a need to know basis where there is an approved business, contractual or legislative need and with the approval of the originator or document owner. · Data must be secured while in the external environment to prevent loss of confidentiality, integrity or availability · You must Encrypt the information either before it's sent, or on the wire between yours and the external environment. - Ensure any documents show the data classification level. · Confirm you are sending to the correct recipient. · Use a standard network transfer protocol such as FTP.

		Highly Confidential	You must only share or send to an external party where there is an approved business need or other justification such as an NDA. · You must only share or send to an external party on a need to know basis where there is an approved business, contractual or legislative need and with the approval of the BT Stakeholder. · You must use full end to end encryption to protect the data from source (your System) to destination (external system) and at rest once it within the 3rd party system in accordance with the requirements in the 3rd Party Standard Section11. - Ensure any documents show the data classification level. · Confirm you are sending to the correct recipient. · Use a standard network transfer protocol such as FTP.
HED120	I want to back-up my electronic documents	All BT data	· You should store BT documents only locations such as network drives or document management systems that have been approved for use by your own INFOSEC team. (If the only option is to use removable media then the device must be encrypted) · All content must be encrypted, or password protected.
HED130	I want to delete electronic documents	All BT data	Documents held in SharePoint and network drives must be disposed of using the standard windows delete function. Recycle bins must be emptied at least once a week. (This does not apply within the Citrix environments e.g. retail back, offshore call centres as this is managed automatically)

			Emails must be deleted when they are no longer required.
HED140	I want to dispose of or re-use IT equipment that has contained confidential/Highly Confidential BT Information e.g. parts, 3rd party equipment, backups, server parts sent back for repair	All BT data	Shredding services can be utilised for many types of media and hardware e.g. HDD, Magnetic tape, Microfiche, CD/DVD, Circuit boards, Mobile telephony You must keep a record of equipment destroyed. Data erasure services can be utilised for equipment that is to be reused. You must a record of equipment where data has been erased and obtain a data erasure certificate. Where equipment has contained UK Government data, Blanco **MUST** be used as this is the only product certified.
HED150	I want to dispose of system and application data	All BT Data	Data must be wiped to a sufficient level so that data is not recoverable. Preferably using Data Erasure (sometimes referred to as data clearing, data wiping, or data destruction) software-based method to overwriting the data. Back-ups that need to be retained for legal and regulatory purposes must be put beyond daily use.

3.4 Handling System & Application data (electronic data).

Electronic data includes all data & information held in systems or applications which are either managed by the Technology department or by individual business units e.g. data warehouse or a billing system. Extracts of data from an application or system received by a person must be treated as an electronic document (see Section 6.3).

Reference	What do you want to do with the data & information	Classification	Handling requirements
HSADE	I want to store and process electronic BT data & information in a data centre (including 3rd Party and Cloud)	All BT information	You must follow the controls in the 3rd Party Standard If data comprises payment card information this must be held in accordance with the PCI DSS requirements. If the data comprises Bank Account Data, because it is especially sensitive the following controls will also apply. 1. Bank accounts must be tokenised for individuals (personal bank accounts of customers and employees). 2. If displaying the actual bank account details to an agent as part of a business process (e.g. to verify the correct account to bill against, or when communicating with a customer e.g. via email, or on an invoice) you must only show the last 4 digits of the bank account (i.e. masked bank account details). 3. If there is a need to access the full bank account (e.g. to enable a credit or debit request from a bank) the bank details must be de-tokenised or decrypted and then passed to the bank using an encrypted transport mechanism. Immediately after use the unencrypted or de-tokenised bank details must be securely deleted.

HSAD1	I want to store and process BT electronic data & information in a 3rd party system or application	All Data	· All Confidential/Highly confidential and Personal information must be encrypted. · Payment Card Information – must be encrypted in accordance with PCI DSS requirements.
HSAD2	I want to send electronic data & information within 3rd party network or externally	All BT Data	Material must have BT Stakeholder approval to be released 3rd party must have an NDA or suitable contract in place. Data transfer must be encrypted. Where Confidential/Highly confidential information including personal data, is to be sent outside your network to a 3rd party, a 'Data Processing Agreement' must be put in place.

4. Information retention.

3rd Party should have a 'Data Retention Policy' supporting this will be specific "Information Retention Schedule" where retention periods must be defined for the BT information being retained. (Retention period should be 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.)

BT information - in whatever form it is held, digitally or in hard copy records and non-records such as all working copies, drafts, informal notes, junk emails or other storage forms (examples are microfiche / microfilm, photographic film, audio or video tapes).

5. Equipment Disposal.

Any equipment that can store data including computer components must be treated as an Information Asset. Examples of 'Information Assets' can be found in the Glossary below.
All equipment must be disposed of at the end of its operational life. Examples of end of life are as follows:

- It's faulty
- It's been decommissioned (service retired or no longer required)
- It's been used in a trial or proof of concept

5.1 3rd party Disposal Requirements.

This applies to:

- Any 3rd party or sub-contracted agencies.
- Any 3rd party who performs maintenance services on BT equipment where information assets may be removed and replaced as part of that service.
- Any 3rd party who provides outsourced services to BT where BT data resides in the 3rd party equipment or archives.
- Any waste disposal agency disposing of BT equipment.

Reference	What do you want to do with the data & information	Classification	Handling requirements
EDR10	I want to dispose of equipment holding BT Data.	All BT Data	Hard Disk Drives (HDD) - Multi Pass Pattern wiping, disintegration or incineration
			Solid State Disk Drives (SSD) - Multi Pass Pattern wiping, disintegration
			CD-R / DVD-R, CD-RW / DVD-RW, BD-R, BD-RE, BD-RE - Abrasion, disintegration, incineration
			Magnetic Tape - Degaussing, disintegration, incineration
			Flash Disk Drives and USB - Multi Pass Pattern wiping, Degaussing, disintegration
			SIMS - Cut into multiple pieces (through the metal contact) to render them unreadable.

6. Audit Requirements.

6.1 Data & Information disposal audit requirements

Full records of data retention and disposal must be kept, providing audit trail, evidence and tracking. This must include:

- Proof of destruction and/or disposal (including date undertaken and method used)
- System audit logs for deletion.
- Data disposal certificates.
- Who undertook the disposal (including any disposal partners / 3rd party's or contractors)?
- A destruction and verification report must be generated to confirm the success or failure of any destruction / deletion process. (i.e. an overwriting process must provide a report that details any sectors that couldn't be erased).

6.2 Equipment disposal audit requirements

An audit trail must be provided for the following equipment types:

- Removable media.
- Disk Drives.
- Back-up tapes.
- Computer components (See Glossary).

Full records must exist to provide an audit trail to include as a minimum:

- The name of the application or service that utilised this piece of equipment.
- Equipment type e.g. desktop, laptop, server, tape, router etc.
- Number of hard drives the equipment contains (if applicable).
- Equipment identified by serial number.
- Component parts of equipment identified by serial number.
- Full asset tracking of all equipment and component parts through the entire equipment disposal lifecycle.
- Proof of destruction and/or disposal (including date undertaken and method used)
- Details of who undertook the disposal (including any disposal partners / 3rd party's / waste disposal contractors).
- A destruction and verification report must be generated that confirms the success or failure of any recycling/sanitisation or destruction process. For example, an overwriting process must provide a report that details any sectors that couldn't be erased. These reports should include the capacity, make, model and serial number of the media.

7. Glossary.

Term	Explanation
3rd parties	Any company involved in processing BT data/information and handling BT equipment must comply with this standard. This includes: · Any 3rd party or sub-contracted agencies · Any 3rd party who performs maintenance services on BT equipment where information assets may be removed and replaced as part of that service · Any 3rd party who provides outsourced services to BT where BT data resides in the 3rd party equipment or archives · Any waste disposal agency disposing of BT equipment
AES	Advanced encryption standard
Asymmetric keys	Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key.
BT data	Any data is owned or licensed by BT to operate as a limited company in the UK or one of its global subsidiaries.

CDP	Certificate Revocation List Distribution Point
CESG	The UK Government Communications-Electronics Security Group.
computer components	Hard disk controllers, CDROM drive controllers, DVD drive controllers, Ethernet interface cards, computer screen controllers and network printers.
CRL	Certificate Revocation List
customer	A person or organisation that obtains, has obtained, or is considered by BT or its brands likely to obtain products, or receive offers for products or services.
customer data	Any data pertaining to customers of the brands operated by BT.
data	Words, numbers, dates, images, sound etc. without context.
data disposal	Data disposal is the destruction of all data and information that is not classified as a permanent record.
data lifecycle	The data lifecycle covers how data is collected, stored, handled, processed, transmitted and destroyed.
data retention period	This is the period (which could be permanent) that a type of data or information is held/stored before it can be destroyed or disposed. During this period that data could be archived if it remains accessible up to the end of the data retention period.
DEK	data encryption key
electronic data	Electronic data is defined as all data & information held in systems or applications which are either managed by the Technology department or by individual business units, e.g. data warehouse or a billing system.
Elliptic-curve Keys	Elliptic-curve cryptography. Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security
encryption	Converting data into a secret code so it can't be read by an unauthorised person.
Entropy	A measure of the randomness of data; 128-bit key may have a maximum of 128 bits of entropy, or as few as 1.
GCM	Google cloud messaging
HSMs	Hardware security modules
inactive record	A record can have an active or inactive state. When an active record is expired or is no longer required, for example when a customer leaves BT- their customer record becomes inactive; or an employee leaves BT and their HR record becomes inactive.
information	A collection of words, numbers, dates, images, sounds etc. put into context i.e. to give them meaning.

information asset	Any equipment that can store data is defined as an 'Information Asset'. Examples include the following: Disk drives (solid state and magnetic), removable media (e.g. floppy disks, USBs, DVDs, CDs, internal memory cards, flash cards & SD cards), backup tapes, mobile phone SIM cards. Computer components such as Hard disk controllers, CDROM drive controllers, DVD drive controllers, Ethernet interface cards, computer screen controllers and network printers.
information systems	A collection of hardware, software, data, people and procedures that work together to produce quality information.
KEK	key encryption key
NDA	Non-disclosure agreement
NIST	National institute of standard and technology
Nonce	A random number generated and used only once during a cryptographic exchange, often for authentication.
non-records	Duplicates of originals and working copies. General documents relating to non-commercial matters. Drafts letters, reports, worksheets and informal notes. Books, manuals, and other printed materials obtained from sources outside of BT for reference material. Spam and junk mail.
OCSP	Online Certificate Status Protocol
office	Relates to any BT premises i.e. retail store, call centre, head office, switch site.
payment card information	Is information relating to an account that is used by a cardholder to make payments to a merchant – examples include but limited to payment account number (PAN), expiry date, CVV. This is governed by the PCI/DSS regulation.
personal data	Information relating to any individual - including but not limited to full name, date of birth, address, telephone number, which includes customers and anyone who works for BT.
PRNG	Pseudo-random number generators
records	Documents kept as evidence of BT business transactions, decisions, activities, emails or as a result of legal obligations. This also includes data and information held in systems or applications as they also contain evidence of EE business transactions, products and services.
RSA	A public-key encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman
Salted hashes	In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. For more information refer to appendix c.
Symmetric keys	Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.
system level retention policy	A system level policy details how long a system holds data to comply with the company Data Retention Schedules

TPM	Trusted Platform module

8. Change History.

Version no	Date	Change made by	Brief details of change
4.0 draft	05/08/18	Karen Tanner	Draft to replace current version 3
4.0 issued	07/11/19	Karen Tanner	Reviewed and signed off
4.0a	20/04/20	Karen Tanner	Henceforth “Internal” will now be known as “General”

9. Document Sign off.

Name	Role	Date
Ian Morton	BT version Document owner	07/11/19

10. Compliance.

We appreciate the vast majority of 3rd party’s act professionally and in line with BT’s Values but if you behave in a way that’s inconsistent with this standard or any other policy or standard, we may terminate the arrangements we have with you for your services.

11. Ownership & Confidentiality.

This document must not 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 must be returned if requested