Annex 1 - Information Classification

Introduction

Within BT all data and information has a BT business owner who is responsible for classifying the document or data.

Data and information must be protected by all users who come into contact with it. As a user of BT information you are responsible for conforming to the security classification controls in this document and any specific project requirements specified by BT. You should only use the document or data for its intended purpose and gain approval from the data owner if you want to allow more people to access it.

If you receive BT information that has not been classified you should contact the sender or your BT manager to confirm the classification, otherwise contact BT Security as per Security Requirements Annex 3.

N.B. If you have access to the BT Greenside Local Area Network (LAN) or are required to create documents for BT that will include any BT information then you need to refer to Security Policy 4 otherwise the following will apply

Information Classifications

There are 4 classifications of information:

- Public
- Internal
- In confidence
- In strictest confidence

Public

Public information does not need control, or is intended for public consumption.

Internal

Internal information is available to BT people and other people who have access to BT's information network, and where such access results in little business risk to BT.

In Confidence

In Confidence information has a specific audience: the need-to-know principle (access controls) is strictly enforced. The unauthorised disclosure of In Confidence information may affect BT's reputation or be harmful to people.

Examples include:

- Personal information about individuals, either BT people, third parties or customers;
- System log data;
- Sales and marketing data;
- Local business plans;
- Risk data;
- Passwords.
- Information that is legally confidential

Collection of multiple In Confidence documents

If you have a collection of In Confidence documents in one location the classification may need upgrading and this may lead to the re-classification of individual documents as In Strictest Confidence or require additional security measures to secure the location if:

- Together they could cause exceptional harm to BT if they were leaked;
- When used with other data item combinations e.g. name and address and/or where multiple bank detail records exist in a system, they could be an attractive target.

If you have concerns about the information in your possession please speak to your BT contact.

In Strictest Confidence

In Strictest Confidence information or data has a defined and small-in-number circulation; the need-to-know principle is strictly enforced (you must know who has copies and who has access). Unauthorised disclosure could cause exceptional harm to BT. You should consider carefully if information is In Strictest Confidence because it requires the most stringent security controls.

Security Controls

Defined Terms:

Encryption

Minimum requirements:

- Use AES 256 bit encryption.
- Symmetric keys must have a minimum key length of 256 bits.
- Asymmetric keys (e.g. RSA) must have a key length of at least 2048 bits.
- Use only known and trusted cryptographic ciphers.
- Do not use Self-signed certificates.

Password/Pass Phrase – (for encryption)

Must not be easily guessable (i.e. be as random as possible, not related to the userid, users, identity, date etc.), and not be discoverable using dictionaries of commonly used passwords. However as a minimum they must be:-

- At least 8 characters long.
- Contain at least two of the following
    - Non-alpha numeric e.g. (!, £,", $, %,^, &,*, (,), -,_, +, =, :, `, @, ~, #, ?, <, >,)
    - Decimal number: (0... 9)
    - Capital case letter: (A... Z)
- Private keys must be protected with a passphrase using a mixture of alpha-numeric characters and symbols as defined above.

NB: For avoidance of doubt any customer specific contractual requirements contained in a Customer contract that require a higher level of security will take precedent over the following controls.

	Security Controls	Internal	In Confidence	In Strictest Confidence
1	**National Data Protection legislation- Personal and Sensitive Personal Data**	Must not be treated as Internal. Protect individual records as In Confidence.	Protect individual records as In Confidence.	Protect bulk records as In Strictest Confidence.
2	**Business document (Word, Excel, etc.) distribution control and movement tracking**	Control and tracking not required. Put the "**BT INTERNAL**" marking on every page, or "**OPENREACH INTERNAL**" if this is only to be shared in Openreach.	Put "**IN CONFIDENCE**" on every page of the document and make sure you follow the "**need to know principle**", and consider the use of a **distribution list.** **Encryption required as per defined terms "Encrypt" and "**Password/Pass Phrase**" above.**	Put "IN STRICTEST CONFIDENCE" on every page of the document. Include a **distribution list** of people within the document. The owner must make sure the "**need to know principle**" is followed. **Encryption required prior to storage using software that complies with the defined terms "Encrypt" and "**Password/Pass Phrase**" above when** data is not stored on a BT provided PC/Laptop with hard disk encryption i.e. removable media. The same applies when you email it to anyone, BT or non-BT.
3	**Secure storage on: laptop and PC**	Secure storage is required e.g. PGP, WinZip 9.	Whole disk encryption **as per defined terms "Encrypt" and "**Password/Pass Phrase**" above.**	Whole disk encryption **as per defined terms "Encrypt" and "**Password/Pass Phrase**" above.**
4	**Secure storage on server and databases (fixed - disk/tape)**	Secure storage not required if compliant with all the physical requirements of the SBCA appendix otherwise Secure storage is required e.g. PGP, WinZip 9	BT Information must be encrypted **as per defined terms "Encrypt" and "**Password/Pass Phrase**" above**.	BT Information must be encrypted **as per defined terms "Encrypt" and "**Password/Pass Phrase**" above.**

5	**Secure storage on Blackberry, Windows Mobile, other PDAs, tablets (iPads etc.), mobile phones and MP3 players**	It is prohibited to store Internal information on such devices unless the device is supplied by BT or a concession is approved by BT Security. Such devices must not be configured to access to BT.com email accounts (access to bt.com email via webmail is permitted).	It is prohibited to store In Confidence information on such devices unless the device is supplied by BT or a concession is approved by BT Security. Such devices must not be configured to access to BT.com email accounts (access to bt.com email via webmail is permitted).	It is prohibited to store ISC on such devices.
6	**Secure storage on:** **Removable media such as memory stick, flash memory, CD/DVD, USB hard drives, secure digital cards, floppy disks and other similar devices.**	BT Information must be encrypted when stored on such devices **as per defined terms "Encrypt" and "**Password/Pass Phrase**" above**.	BT Information must be encrypted when stored on such devices **as per defined terms "Encrypt" and "**Password/Pass Phrase**" above.**	It is prohibited to store ISC on such devices.
7	**Web/on-line storage or any Internet storage facility**	Prohibited	Prohibited	Prohibited
8	**External Web collaboration**	Any MS LiveMeeting platform or Webjoin	Prohibited	Prohibited
9	**Sent via email**	Encryption not required.	Encrypted for recipients (where the destination is not a bt.com email) **as per defined terms "Encrypt" and "**Password/Pass Phrase**" above.**	**Encryption required as per defined terms "Encrypt" and "**Password/Pass Phrase**" above.**
10	**Email auto-forwarding**	Prohibited	Prohibited	Prohibited
11	**Network Transmission**	Encryption not required.	Encrypted for external and internal transmission, **as per defined terms "Encrypt" and "**Password/Pass Phrase**" above.**	Encrypted for external and internal transmission, **as per defined terms "Encrypt" and "**Password/Pass Phrase**" above.**
12	**File transfer**	Use secure file transfer e.g. SFTP, XFB.	Use secure file transfer e.g. SFTP, XFB.	Use secure file transfer e.g. SFTP, XFB.

13	**Data erasure/deletion**	Use application or operating system deletion facilities.	Sanitise data by overwriting every sector with random binary strings at least once using a software product e.g. Blanco HMG Edition or Blanco Version 5 if using Solid State Devices.	Sanitise data by overwriting every sector with random binary strings at least once using a software product e.g. Blanco HMG Edition or Blanco Version 5 if using Solid State Devices.
14	**Disposal or re-use of IT equipment ((holding BT Information)** **Including but not limited to:** **- Disposal of parts** **- Destruction of Supplier equipment** **- Destruction requirements for backups** **- Server parts that are sent back to manufacturer for repair**	Use a verifiable and tested software erasure solution where a formal certificate is produced to verify erasure. Any equipment that fails to erase must be destroyed and a formal certification received/provided with at least a record of the serial number of the equipment as proof of disposal. The solution above cannot be used with Solid State Drive (SSD's) which must be destroyed and formal certification received/provided. Refer to BS EN 17513 for further information.	Disks (or other storage media including but not restricted to compact flash, solid state device) must be sanitised by overwriting every sector with random binary strings at least once using a software product e.g. Blanco HMG Edition or Blanco Version 5 if using Solid State Devices. If sanitisation cannot be achieved or is not appropriate then the disk (or other storage media including but not restricted to compact flash, solid state device) must be destroyed using a disk destruction facility. A formal certificate must be produced to verify erasure or destruction.	Disks (or other storage media including but not restricted to compact flash, solid state device) must be sanitised by overwriting every sector with random binary strings at least once using a software product e.g. Blanco HMG Edition or Blanco Version 5 if using Solid State Devices. If sanitisation cannot be achieved or is not appropriate then the disk (or other storage media including but not restricted to compact flash, solid state device) must be destroyed using a disk destruction facility. A formal certificate must be produced to verify erasure or destruction.
15	**Printing**	Use a printer connected to the PC or be present at network printer whilst printing.	Use a PIN controlled printer or printer connected to the PC, or a printer in an access controlled room. Double check which printer it's going to and don't leave documents in the print tray.	Use a PIN controlled printer or printer connected to the PC, or a printer in an access controlled room. Be careful when you're printing. Double check which printer it's going to and don't leave documents in the print tray.

16	**Postal/courier services between BT and the Supplier**	Single envelope.	Use double envelopes and send by recorded delivery to addressee only and do not mark as "In confidence" on the 1st envelope.	Use double envelope and send by recorded delivery addressee only and do not mark as "In Strictest confidence" on the 1st envelope.
17	**External Disclosure**	Seek authority from BT Security contact. Refer to Annex 3.	Seek authority from BT Security contact. Refer to Annex 3.	Seek authority from BT Security contact. Refer to Annex 3.
18	**Used in training, development or testing**	Must be anonymised by BT and comply with BT's Data anonymisation best practice guide BP001.	Must be anonymised By BT and comply with BT's Data anonymisation best practice guide BP001.	Prohibited
19	**Paper disposal**	Shredded using cross cut shredders.	Shredded using cross cut shredders.	Shredded using cross cut shredders to 4 x 15 mm.
20	**Public areas**	Do not talk about Internal Information in public.	Do not talk about In Confidence Information in public. Do not work on documents in public spaces where you can be overlooked.	Do not talk about In Strictest Confidence Information in public. Do not work on documents in public spaces.