3rd Party Information Classification & Handling Specification

Introduction

Not all information has the same value or sensitivity and classifying it helps us work out how it should be protected; demonstrates our commitment to that protection and helps us handle it efficiently.

We have four classification levels:

- Public
- Internal
- In Confidence
- In Strictest Confidence

How Do I Handle the Data?

Once the classification has been notified, the data must be handled according to the classification level so it's properly protected, whether it's on a computer, travelling across a network, written down or spoken. By default any information provided by BT will be classified as In Confidence unless otherwise stated. For avoidance of doubt personal data is classified as In-Confidence as a minimum. (personal data' means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity)

We have rules for handling data and information.

- **Spoken and multimedia** e.g. talking, social networking, texting, skyping
- **Paper documents** e.g. printing, posting, disposing
- **Electronic documents** e.g. saving, emailing, transferring, deleting
- **In applications or systems** e.g. external data Centre's

If you receive BT information that has not been classified you should contact the sender or your BT contact to confirm the classification.

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.

Handling Spoken & Multimedia Data

Ref	What do you want to do?	Classification	Handling Requirements	Reason
HSM10	I want to post information on social media / networking sites – e.g. personal Twitter account	Public	You must not contribute to sites or post online statements that could be reasonably attributed as the views of BT or are defamatory to BT, and might cause harm to BTs brand and reputation.	Unauthorised release of information or personal comment could damage our brand
		Internal	Not allowed	
		In Confidence	Not allowed	
		In Strictest Confidence	Not allowed	
HSM20	I want to discuss or present something via internal	Internal	You can use Live Meeting, WebEx, Webjoin, and Lync/Skype for Business	Internal data can be seen by people invited to the meeting

	conferencing or messaging	In Confidence	You can use Live Meeting, WebEx, Webjoin, and Lync/Skype for Business	IC data can be seen by people invited to the meeting
		In Strictest Confidence	• You can use the BT hosted Lync/Skype for Business • You must verify who is on the conference • You must lock the conferencing meeting so no-one else can join	Lync/Skype for business encrypt using (256-bit AES) data
HSM30	I want to discuss something 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 website	To prevent unauthorised disclosure of information
		Internal	Not allowed	
		In Confidence	Not allowed	
		In Strictest Confidence	Not allowed	
HSM40	I want to discuss something via face to face/phone call	Internal	Make sure the conversation can't be overheard by anyone not working for or on behalf of BT	To prevent unauthorised disclosure of information
		In Confidence	As 'Internal' and • Verify the identity of the person you are talking to and confirm they have 'a need to know' before discussing anything confidential • Make sure a contract is in place with relevant 3rd parties before starting the conversation, if applicable (NB. Before assigning or subcontracting the whole or any part of the contract to a 3rd party you must obtain BT's prior written consent) • Make sure the conversation can't be overheard • Do not leave 'In Confidence' information on voicemail systems	To protect confidential information and make sure it's restricted to those who need to know
		In Strictest Confidence	As 'In Confidence' and • Keep any 'In Strictest Confidence' information to the absolute minimum	
HSM50	I want to send a message/content via SMS/MMS to all parties (internal & external)	Public	Message content must be restricted to 'public information' available on our website	To prevent unauthorised disclosure of information
		Internal	No special handling requirements	
		In Confidence	Make sure the message is only sent to those who need to know and the following must not be disclosed: • Payment card information • Bank details • Password details	These 3 items are In Strictest Confidence

		In Strictest Confidence	Not allowed

Handling Paper Documents

Ref	What do you want to do?	Classification	Handling Requirements	Reason
HPD10	I want to work on hard copy information in 3rd party premises or at home	Internal	You must apply the clear the desk policy when away from your desk	To prevent accidental disclosure
		In Confidence	As 'Internal' and • When not working on the documents, put out of sight and lock away.	
		In Strictest Confidence	As 'In Confidence'	
HPD20	I want to print	Internal	• Check you're sending to the right printer • Don't leave documents in the print tray	To prevent accidental disclosure
		In Confidence	As 'Internal' and • Use an access controlled printer, a printer connected to a PC, or a printer in an access controlled room	
		In Strictest confidence	As 'In Confidence'	
HPD30	I want to use a printer which isn't in either a Supplier Building or at my home (e.g. it's in 3rd party premises, a hotel etc.)	Internal	This is normally not allowed because printers have memories and data can be retrieved from them. Use your common sense – do you really want other people to see this information?	Data and information can be retrieved from a printer's memory
		In Confidence	Not allowed	
		In Strictest Confidence	Not allowed	
HPD40	I want to carry hardcopy information outside of my place of work	Internal	Carry in an opaque folder or bag	To protect against accidental disclosure
		In Confidence	As 'Internal' and • You must not remove customer and/or payment data from Supplier offices	
		In Strictest Confidence	As 'In Confidence'	
HPD50	I want to share or send hardcopy information to internal parties	Internal	• Place in an envelope and use the internal post.	Guards against casual observation
		In Confidence	• Don't mark 'In Confidence' on the outside envelope. • If the information is covered by 'legal privilege' seek	Prevents casual observers being aware the contents are In Confidence. Signed for delivery provides proof of posting, signature on

			guidance from your legal team.	delivery and online confirmation of delivery of the item
		In Strictest Confidence	• Use 2 envelopes and send using a 'tracked' delivery • Don't mark the outside envelop 'In Strictest Confidence' • Get the permission of the document owner to share the hardcopy • Preferably share by hand to authorised named individuals • Associate copies with individuals by watermarking with a name or number (if available) • If lost you must raise a security incident	Prevents casual observers being aware the contents are In Strictest Confidence. Signed for delivery provides proof of posting, signature on delivery and online confirmation of delivery of the item
HPD60	I want to share or send hardcopy to external parties	Internal In Confidence In Strictest Confidence	Make sure you have a contract in place as per HSM40 with relevant 3rd parties. Then then the controls are the same as for sharing with internal parties	See HPD50
HPD70	I want to send a fax	Internal	You must make sure a fax header page is included before the content pages(s)	To prevent accidental disclosure
		In Confidence	• You must send a header page with a test page and then contact the recipient to confirm receipt before faxing the content • If the information is covered by 'legal privilege' seek guidance from your legal team	To prevent unauthorised people receiving information
		In Strictest Confidence	Not allowed	
HPD80	I want to dispose of hardcopy information	Internal	You must • shred it or • put in a document bin which it can't be taken out of easily	General waste and/or recycling bins are not safe forms of disposal
		In Confidence	You must shred it to a minimum Particle size ≤ 160MM^2 and for regular particles strip width ≤ 2MM e.g. 2X15 mm.	To protect 'In Confidence' information from disclosure
		In Strictest Confidence	You must shred it to a minimum Particle size ≤ 160MM^2 and for regular particles strip width ≤ 2MM e.g. 2X15 mm using a cross cut shredder	To protect 'In Strictest Confidence' information from disclosure

Handling Electronic Documents

Ref	What do you want to do?	Classification	Handling Requirements	Reason
HED10	I want to store electronic information	Internal	Full disc encrypt using (256-bit AES) encryption.	This converts information into unreadable code

	on my business laptop/PC			which can’t be deciphered easily by unauthorised people.
		In Confidence	Full disc encrypt using (256-bit AES) encryption.	
		In Strictest Confidence	Full disc encrypt using (256-bit AES) encryption.	
HED20	I want to store my documents on SharePoint or another document management system that is NOT hosted in the cloud or with internet Services	Internal	• Use permission levels and groups to set up role based access control. These must set to no more than the minimum for people to do their jobs • Review the access controls each year	Restricts access and/or editing to those who need to know
		In Confidence	As ‘Internal’ and • Document the process for assigning people to roles. • The roles and people assigned to them must be reviewed every 90 days • Documents must be encrypt using (256-bit AES) with Winzip_before uploading	
		In Strictest Confidence	As ‘Internal’ and • Document the process for assigning people to roles. • The roles and people assigned to them must be reviewed every 90 days • Documents must be encrypt using (256-bit AES) with Winzip_before uploading	
HED30	I want to store electronic information in the cloud or with internet Services such as Google docs, GitHub, btcloud.bt.com, Drobox, Pastebin, Facebook etc.	Internal	Not allowed.	Internet services increase the risk of unauthorised access to information
		In Confidence	Not allowed.	
		In Strictest Confidence	Not allowed.	
HED40	I want to store electronic information on removable media e.g. a memory stick.	Internal	• USB devices must be encrypt using (256-bit AES) with ‘BitLocker To Go’ • Non Windows machines: ‘BitLocker to Go’ doesn’t work on non-Windows machines so not allowed Under no circumstances may personal data be stored on these devices unless encrypted using (256-bit AES).	Removable media can be lost or stolen more readily than a whole computer and so the risk of unauthorised people accessing data is higher. To protect the information it must be converted into unreadable code which can’t be deciphered easily by unauthorised people
		In Confidence	As ‘Internal’	
		In Strictest Confidence	As ‘internal’	
HED50	I want to store electronic documents	Internal	Not allowed	Unauthorised people may be able to

	or BT information on my personal laptop or device			access to BT data especially if the device is lost, stolen, discarded in favour of a newer model.
		In Confidence	Not allowed	
		In Strictest Confidence	Not allowed	
HED60	I want to send electronic documents or information to my personal email address	Internal	Not allowed	To prevent disclosure to non –authorised people
		In Confidence	Not allowed	
		In Strictest confidence	Not allowed	
HED70	I want to auto-forward to an external email address	Internal	Not allowed	Data could be accessed by unauthorised people if the email account, the ISP or internet connection is compromised
		In Confidence	Not allowed	
		In Strictest confidence	Not allowed	
HED80	I want to *internally* share or send electronic information by email	Internal	No special requirements	
		In Confidence	• Make clear the email is 'In Confidence' • Use sensitivity settings to mark the email as 'Confidential' • Ideally set the permissions to 'Do not forward' • If the information is covered by 'legal privilege' seek guidance from your legal team • Use Secure email to send • If secure email isn't possible you must encrypt using (256-bit AES) the file before sending • Set the permissions to 'Do not forward'	To retain control over confidential information
		In Strictest confidence	As 'In confidence'	To protect the information while in transit across networks
HED90	I want to *externally* share or send electronic information by email	Internal	You can only send to an external party if you have a contract in place as per HSM40	To retain control over confidential information
		In Confidence	As 'Internal' and • Encrypt using (256-bit AES) • Confirm you're sending to the correct email address • If the information is covered by 'legal privilege' seek guidance from your legal team	
		In Strictest confidence	As 'In Confidence'	
HED100	I want to internally transfer a document or information not	Internal	No special handling requirements. Use an internal file transfer facility.	
		In Confidence	As 'Internal' and with encryption	

	using email, Skype/Lync for Business or removable media. (e.g. because the file is too large)		• If the information is covered by 'legal privilege' seek guidance from your legal team • Encrypt the file at source using (256-bit AES) before uploading to the file transfer facility.	
		In Strictest Confidence	As "In-Confidence	To protect the information when in transit across the network and after delivery
HED110	I want to externally transfer a document or information not using email, Skype/Lync for Business or removable media (e.g. because the file is too large)	Internal	You can only send to an external party if you have a contract in place as per HSM40. • Confirm you are sending to the correct recipient • Use a standard network transfer protocol such as FTP or a Gateway such as SDEDS	
		In Confidence	As 'Internal' and • You must encrypt using (256-bit AES) the information at source before transferring – via a Gateway such as SDEDS • If the information is covered by 'legal privilege' seek guidance from your legal team	SDEDS provides a secure tunnel for transferring the data, but it must be encrypt using (256-bit AES) before send so that it remains encrypt using (256-bit AES) after delivery.
		In Strictest confidence	As 'In Confidence''	
HED120	I want to back up my electronic documents	Internal	• You must store your documents on Supplier's network drives or Suppliers document management system, as per HED030. • The backed up document must be protected to the same level as on the network drive, SharePoint. • If you use removable media then the device must be encrypt using (256-bit AES).	Backups must have the same level of classification & protection as the original data
		In Confidence	As 'Internal' and • Encrypt the document using (256-bit AES) before backing up	
		In Strictest confidence	Back them up to removable media which is encrypted using (256-bit AES).	
HED130	I want to delete electronic documents from PC/Laptop or document management system.	Internal	Use the application or system deletion facility. Empty the recycle bin periodically	Some data may remain even after a file has been erased/deleted or the disk formatted.
		In Confidence	As 'Internal' legal team	
		In Strictest confidence	As 'Internal'	

HED140	I want to dispose of or re-use IT equipment e.g. parts, supplier equipment, backups, server parts sent back for repair.	Internal	You must ensure that data is irretrievable destroyed. As a minimum 3 passes with random binary characters.	This makes sure the data is irretrievable.
		In Confidence	As ‘Internal’	
		In Strictest confidence	As ‘Internal’	

Handling System & Application data

Ref	What do you want to do?	Classificatio n	Handling Requirements	Reason
HSADE	I want to store and process electronic data & information held in an external data centre	Internal	No special requirements if compliant to all applicable requirements above for storing data for this classification.	
		In Confidence	You must follow 3rd party External data hosting Requirements http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	
		In Strictest confidence	As ‘In Confidence’	