

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

The below table provides guidance on the types of information that will fall into each of these four categories.

By default any BT Information will be classified as In Confidence unless otherwise stated.

If you are unsure which category information falls into please contact your BT Security Contact.

Classification	Overview Description	Examples
Public – Cat 1	Public information is information that is available to both people inside and outside of BT.	<ul style="list-style-type: none"> • Advertising campaigns. • Generic communications already in the public domain (e.g. PR statements, public articles about BT) • Publically available commercial information such as published prices or offers
Internal – Cat 2	<p>BT information that is available to BT people and other people who have access to BT's information network, and where such access results in minimal business risk to BT.</p> <p>Internal information may include information that is subject to general obligations of confidentiality (e.g. business-as-usual emails, reports or contractual documents), provided that that information is not sufficiently commercially sensitive to require the enhanced protections described below.</p>	<ul style="list-style-type: none"> • Internal newsletters such as BT News • FixIt articles • General non-sensitive emails (e.g. no commercial information or limited personal data as detailed in column on left contained in the body of the email)
In Confidence – Cat 3	In Confidence information is information that should be limited to a specific audience and where the unauthorised disclosure of the information may damage BT's reputation or its disclosure would potentially be harmful to the people the information it concerns (e.g. most personal data about employees or customers). The need-to-know principle should be applied to In Confidence information.	<ul style="list-style-type: none"> • System log data; • Commercially sensitive sales and marketing data; • Local business plans; • Most personal data; and • Risk data. • All Personal Data (as defined in the Condition headed "Protection of Information") unless it classified as In-Strictest Confidence below.

	<p>Collection of multiple In Confidence documents</p> <p>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:</p> <ul style="list-style-type: none"> • Together they could cause exceptional harm to BT if they were leaked; or • When used with other data item combinations they could be an attractive target. 	
<p>In Strictest Confidence – Cat 4</p>	<p>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.</p>	<ul style="list-style-type: none"> • Bank account details • Authentication details should be treated as In Strictest Confidence. • Computer passwords, passwords must be stored and secured in accordance with BT's Cryptography Specifications • Financial accounting data under embargo until the publication of the annual report • Strategic business plans, competitive strategy, new strategic products, and new marketing policies • Very sensitive competitor, partner or contractor assessments • Sensitive HR information which may alienate a significant number of employees • Details of major acquisition, alliance, divestment and merger plans • Details about significant network vulnerabilities • Customer security codes, master encryption codes, key calculations, transaction, account, or audit details • customer security codes, master encryption codes, key calculations, transaction, account, or audit details • Audit reports or findings containing details of serious shortcomings/vulnerabilities in BT practices or processes

How Do I Handle the Data?

Information 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.

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. data Centre's

We also have separate guidelines on the level and type of encryption we expect to be used to protect information (our "Encryption Standard").

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 conferencing or messaging	Internal	You can use Live Meeting, WebEx, Webjoin, and Lync/Skype for Business	Internal data can be seen by people invited to the meeting
		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	<ul style="list-style-type: none"> • 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 as per the Encryption Standard below 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 <ul style="list-style-type: none"> • 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 	To protect confidential information and make sure it's restricted to those who need to know

PUBLIC DOCUMENT

			<p>or subcontracting the whole or any part of the contract to a 3rd party you must obtain BT's prior written consent)</p> <ul style="list-style-type: none"> • Make sure the conversation can't be overheard • Do not leave 'In Confidence' information on voicemail systems 	
		In Strictest Confidence	<p>As 'In Confidence' and</p> <ul style="list-style-type: none"> • 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	<p>Make sure the message is only sent to those who need to know and the following must not be disclosed:</p> <ul style="list-style-type: none"> • 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	<p>As 'Internal' and</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Check you're sending to the right printer • Don't leave documents in the print tray 	To prevent accidental disclosure
		In Confidence	<p>As 'Internal' and</p> <ul style="list-style-type: none"> • Use an access controlled printer, a printer connected to a PC, or a printer in an access controlled room 	

PUBLIC DOCUMENT

		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 <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Place in an envelope and use the internal post. 	Guards against casual observation
		In Confidence	<ul style="list-style-type: none"> Don't mark 'In Confidence' on the outside envelope. If the information is covered by 'legal privilege' seek guidance from your legal team. 	Prevents casual observers being aware the contents are In Confidence. Signed for delivery provides proof of posting, signature on delivery and online confirmation of delivery of the item
		In Strictest Confidence	<ul style="list-style-type: none"> 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	Make sure you have a contract in place as per HSM40 with relevant 3 rd parties. Then then the controls are the same as for sharing with internal parties	See HPD50
		In Confidence		
		In Strictest Confidence		
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	<ul style="list-style-type: none"> You must send a header page with a test page and then contact the recipient to confirm receipt before faxing the content 	To prevent unauthorised people receiving information

			<ul style="list-style-type: none"> If the information is covered by 'legal privilege' seek guidance from your legal team 	
		In Strictest Confidence	Not allowed	
HPD80	I want to dispose of hardcopy information	Internal	You must <ul style="list-style-type: none"> 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 $\leq 160\text{MM}^2$ and for regular particles strip width $\leq 2\text{MM}$ e.g. 2X15 mm.	To protect 'In Confidence' information from disclosure
		In Strictest Confidence	You must shred it to a minimum Particle size $\leq 160\text{MM}^2$ and for regular particles strip width $\leq 2\text{MM}$ 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 on my business laptop/PC	Internal	Full disc encryption used as per the Encryption Standard below.	This converts information into unreadable code which can't be deciphered easily by unauthorised people.
		In Confidence	Full disc encryption used as per Encryption Standard below.	
		In Strictest Confidence	Full disc encryption used as per Encryption Standard below.	
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	<ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 as per the Encryption Standard below 	
		In Strictest Confidence	As 'Internal' and <ul style="list-style-type: none"> Document the process for assigning people to roles. 	

PUBLIC DOCUMENT

			<ul style="list-style-type: none"> The roles and people assigned to them must be reviewed every 90 days Documents must be encrypted as per the Encryption Standard below 	
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	<ul style="list-style-type: none"> USB devices must be encrypted as per the Encryption Standard below <p>Under no circumstances may personal data be stored on these devices unless encrypted as per the Encryption Standard below.</p>	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 or BT information on my personal laptop or device	Internal	Not allowed	Unauthorised people may be able to 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 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 <i>internally</i> share or send electronic information by email	Internal	No special requirements	
		In Confidence	<ul style="list-style-type: none"> Make clear the email is 'In Confidence' Use sensitivity settings to mark the email as 'Confidential' Ideally set the permissions to 'Do not forward' 	To retain control over confidential information

PUBLIC DOCUMENT

			<ul style="list-style-type: none"> If the information is covered by 'legal privilege' seek guidance from your legal team 	
		In Strictest confidence	<p>As 'In confidence' plus</p> <ul style="list-style-type: none"> Use Secure email to send If secure email isn't possible you must encrypt as per the Encryption Standard below the file before sending Set the permissions to 'Do not forward' 	To protect the information while in transit across networks
HED90	I want to <i>externally</i> 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	<p>As 'Internal' and</p> <ul style="list-style-type: none"> Encrypt as per the Encryption Standard below 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'	
HED120	I want to back up BT's electronic documents	Internal	<ul style="list-style-type: none"> 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 as per the Encryption Standard below. 	Backups must have the same level of classification & protection as the original data
		In Confidence	<p>As 'Internal' and</p> <ul style="list-style-type: none"> Encrypt the document as per the Encryption Standard below before backing up 	
		In Strictest confidence	As 'In Confidence'	

Handling System & Application data

Ref	What do you want to do?	Classification	Handling Requirements	Reason
HSADE	I want to store and process electronic data & information held in a data centre or on a system server	Internal	No special requirements if compliant to all applicable requirements above for storing data for this classification.	
		In Confidence	<ul style="list-style-type: none"> Encrypt as per the Encryption Standard below <p>For a data Centre you must also follow 3rd party External data hosting Requirements http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm</p>	
		In Strictest confidence	<p>As 'In Confidence' plus</p> <p>To protect Bank account data because it is especially sensitive the following controls apply. These take precedence over any other applicable controls in this security specification.</p> <ol style="list-style-type: none"> Bank accounts must be tokenised for individuals (personal bank accounts of customers and BT employees) this excludes BT's own bank account details and the bank details of the various BT legal entities). If an application only holds corporate bank accounts then the 3rd party can make a case (based on time, cost, resource, number of accounts, and number of users with access to the application etc.) as to whether BT will initially accept an encryption based solution. <p>If an encryption based solution is agreed then BT will review the decision when all bank accounts are protected to determine if that is adequate going forward. This will be influenced by the threat levels and the risk appetite of the business as a whole.</p> <ol style="list-style-type: none"> When displaying the actual bank account details to an agent as part of a business process (e.g. to verify that we have the correct account to bill against, or when communicating with a customer e.g. via email, or on an invoice) we must only show the last 4 digits of the bank account (i.e. masked bank account details). 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 compliant with BT 	

			security policy. Immediately after use the unencrypted or de-tokenised bank details must be securely deleted.	
--	--	--	---	--

Encryption Standards

General Cryptography Controls.

Ref	Control	Reason
C1.10	Current Cryptographic libraries must be used	Cryptographic libraries are updated regularly. In addition to updating software packages in-line with vendor direction cryptographic packages should be reviewed and updated regularly.
C1.20	Only use approved industry standard cipher suites for encryption. E.g. for TLS SSLv2	Non approved ciphers may introduce vulnerabilities
C1.30	The latest version of TLS must be used for new deployments. SSL V1,2 & 3 must not be used	Earlier versions, up to and including TLS1.0 are no longer considered secure
C1.40	Perfect Forward Secrecy must be enabled	Perfect forward secrecy algorithms prevent captured messages being decrypted even if the authentication private key is compromised in the future
C1.50	Self-signed certificates must not be used	Self-signed certificates negate the benefit of end-point authentication and also significantly decrease the ability for an individual to detect a man-in-the-middle attack.
C1.60	An industry standard certification authority must be used for certificate management. E.g. verisign	To maintain an inventory of certificates issued for vulnerabilities and certificate expiry
GTS2.370		
C1.70	<p>Passwords must be protected using a non-reversible one way mathematical function (e.g. Hashing algorithm) with a unique randomising factor (Salt) per password.</p> <p>NB. SALT is random data that is used as an additional input to a one-way function that "hashes" a password or passphrase.</p>	Stored password files can be extracted and as such all entries must be protected to prevent recovery of clear text passwords
C1.80	Protected passwords as per C1.70 must be stored away from a system's configuration files and have access control implemented so that only appropriate privileged users can read or copy the contents.	It must never be possible to retrieve protected passwords by directory traversal, SNMP walk, configuration dump, or other mechanism, which might allow attempts at offline cracking.

Technical Cryptography Implementation

SSL/TLS Protocols	
Can Use	Don't use
TLSv1.3 (tbc - Available in OpenSSL after April 5th).	SSLv3.0
TLSv1.2	SSLv2.0
TLSv1.1	
TLS v1.0*	

* TLSv1.0 is already end of life and may be deprecated at any time due to known issues. For compliance reason (for example PCI-DSS) protocols such as TLSv1.0 and TLSv1.1 may have to be turned off. All developers should be ready to disable these protocol by configuration.

Key Sizes			
------------------	--	--	--

	Symmetric	Asymmetric	Elliptical Curve
Brownfield	≥ 112 bits	≥ 2048 bits	≥ 224 bits
Greenfield	≥ 128 bits	≥ 3072 bits	≥ 384 bits

Key Exchange	
Can Use	Don't Use
ECDHE (Ephemeral (temp key) Diffie-Hellman Key Exchange (keys not based on certs))	kRSA (RSA Key Exchange)
	kDHr (Diffie-Hellman Key Exchange with RSA key)
	kDHd (Diffie-Hellman Key Exchange with DSA key)
	kSRP (Secure Remote Password (SRP) Key Exchange)
	kADH (Anonymous Diffie-Hellman key exchange)
	kPSK (Pre-shared Key Key Exchange)

Perfect forward security should be based on locally configured or generated Diffie-Hellman Group values that include "safe" primes.

Diffie Hellman Parameters

Diffie Hellman Parameters	
Can Use	Don't Use
3072-bit Diffie-Hellman Group (best – must be locally generated).	The server default values (generate your own locally)
2048-bit Diffie-Hellman Group (approaching end of life – must be locally generated).	

Authentication	
Can Use	Don't Use
aRSA (RSA Authentication)	aNULL (no authentication)
aECDSA (Elliptic Curve Digital Signature Algorithm Authentication)	aDSS (DSS Authentication)
	aECDH (Elliptic Curve Diffie-Hellman)
	aDH (Diffie-Hellman)
	aDSA (Digital Signature Algorithm)
	aPSK (Pre-shared Key)
	aSRP (Secure Remote Password)

Cipher/Encryption	
Can Use	Don't Use
AES 256 GCM (Rijndael (Advanced Encryption Standard) - Galois Counter Mode)	eNULL (no encryption)
AES 128 GCM (Rijndael (Advanced Encryption Standard) - Galois Counter Mode)	DES (DES encryption)
CHACHA20/POLY1305 (256)	3DES (3DES encryption)
AES 256 CCM (Rijndael (Advanced Encryption Standard) - (Counter Mode with CBC-Mac)	RC4 (RC4 encryption)
AES 128 CCM (Rijndael (Advanced Encryption Standard) - (Counter Mode with CBC-Mac)	RC2 (RC2 encryption)
AES 256 CBC (Rijndael Cipher Block Chaining) – approaching end of life.	IDEA (IDEA encryption)

PUBLIC DOCUMENT

AES 128 CBC (Rijndael Cipher Block Chaining) – approaching end of life.	Seed (Seed encryption)
	Camellia (Camellia encryption)
	ARIA (ARIA encryption)

MAC Digest Algorithm	
Can Use	Don't Use
AEAD (Authenticated Encryption Additional Data)	MD5 (MD5 Hash function)
SHA512 (SHA2 family - SHA512 Hash function)	SHA1 (SHA1 Hash function)
SHA384 (SHA2 family - SHA384 Hash function)	SHA (alias for SHA1)
SHA256 (SHA2 family - SHA256 Hash function)	