Disclosure & Barring Service

TATA CONSULTANCY SERVICES

TCS/DBS Information Classification and Media Handling Policy

Document Reference No:	TCS.04.364
Document Author:	Hatim Lokat *TCS Information Security Consultant*
Document Owner:	George Kuncheria *TCS Client Director* Paul Whiting *DBS Senior Information Risk Owner*
Version:	2.0
Approved Date:	

Document Location

TCS: SharePoint Folder / TCS PMO Folder Repository
DBS: Horizon portal

Document Revision History

The document will be reviewed on an annual basis and/or when changes happen to the TCS/DBS Programme.

No	Description/Reason for Change	Author	Version	Date	Type of Review
1	Initial Draft	Hatim Lokat	0.1	27/04/2015	
2	Incorporating DBS review comments	Hatim Lokat	0.2	07/05/2015	TCS/DBS review
3	Incorporating DBS review comments and updates as per revised SAL	Hatim Lokat	0.3	29/09/2015	TCS/DBS review
4	Incorporating DBS review comments	Hatim Lokat	0.4	09/11/2015	TCS/DBS review
5	Incorporating DBS review comments	Hatim Lokat	0.5	04/12/2015	TCS/DBS review
6	Baselined following DBS approval	Hatim Lokat	1.0	19/01/2016	-
7	Changed / Updated the document reviewers, approvers and owners name and baselined the document.	Hatim Lokat	2.0	16/11/2016	-

Document Reviewers *(those who will review the product)*

No	Name	Organisation/Role	Version	Date of Review
1	Joseph Ball	TCS Head of Security for DBS Programme	0.5	02/12/2015
2	Peter Kendall	DBS Security Operations Manager	0.5	21/12/2015
3	Paul Orlowski	DBS Security Accreditor	0.5	21/12/2015
4	Michelle Anderson	Barring Security	0.5	21/12/2015
5	Elaine Carlyle	DBS Head of Security	0.5	21/12/2015
6	Andrew Watson	DBS Chief Information Officer	0.5	21/12/2015
7	Adele Downey	DBS Senior Information Risk Owner	0.5	21/12/2015
8	Joseph Ball	TCS Head of Security for DBS Programme	2.0	16/11/2016
9	Peter Kendall	DBS Security Operations Manager	2.0	16/11/2016

10	Paul Orlowski	DBS Security Accreditor	2.0	16/11/2016
11	Michelle Anderson	Barring Security	2.0	16/11/2016
12	Elaine Carlyle	DBS Head of Security	2.0	16/11/2016
13	Paul Whiting	DBS Senior Information Risk Owner	2.0	16/11/2016

Document Approvers *(those who have final authority to approve the product)*

No.	Name	Organisation/Role	Version	Date of Approval
1	George Kuncheria	TCS Client Director	2.0	
2	Paul Whiting	DBS Senior Information Risk Owner	2.0	

Document Distribution

This document is a controlled version, which needs to be circulated to the following stakeholders in the organisation whenever new changes are incorporated.

No.	Name	Organisation/Role	Version	Distributed Date
1	All TCS associates working on DBS engagement	TCS	2.0	
2	All DBS associates	DBS	2.0	

Document Classification:

The owner(s) / author(s) of the document have classified it as “OFFICIAL” as per TCS/DBS Data Classification policy and standards. The use of the document shall be as per the classification and consent from owner/author shall be obtained before changing the document classification.

Internal / Informative References

No.	Reference Document
1	ISO/IEC 27001:2013 standards
2	TCS.03.491 TCS Information Classification and Media Handling Policy

Abbreviations

Abbreviation	Description
TCS	Tata Consultancy Service
DBS	Disclosure and Barring Service
GSC	Government Security Classification
HMG	Her Majesty Government
PDR	Personal Development Review
FOI	Freedom of Information
POVA	Protection of Vulnerable Adults
POCA	Public Order and Civil Enquiry
CRM	Customer Relationship Management
FIPS	Federal Information Processing Standard
CPA	Commercial Product Assurance

IS5	INFOSEC Standard
GSi	Government Secure Intranet
PNN	Police National Network
CJX	Criminal Justice Extranet
CJSM	Criminal Justice Secure eMail

1.0 Introduction

1.1 This document provides guidance for all Tata Consultancy Services (TCS) and Disclosure and Barring Services (DBS) staff on the classification of information assets. It additionally provides guidance regarding:

a) The associated handling requirements for media containing classified information.
b) The implementation of protective controls proportionate to the sensitivity of the information to be stored or processed

2.0 Scope

2.1 This policy applies to all information that TCS/DBS collects, processes, stores, generates or shares to deliver services, including information received from or exchanged with external partners or third party suppliers. This document is aligned to the core principles of the UK Government Security Classification (GSC) scheme.

This document covers business data used by TCS/DBS in the context of the DBS service only. Information that is internal to TCS is not covered in this document but is covered under TCS Corporate Information Classification Policy.

3.0 GSC Information Classification Terms

3

3.1 The GSC classification scheme has three categories (in descending order) as defined below:

a) **TOP-SECRET** – HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.
b) **SECRET -** that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.
c) **OFFICIAL -** The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

4.0 TCS/DBS Information Classification

4.1 OFFICIAL Classification

a) All information within TCS/DBS will be managed within the OFFICIAL tier. TCS/DBS will not hold or process any information within TOP-SECRET or SECRET tier
b) The OFFICIAL classification covers the vast majority of information which will be handled by TCS/DBS staff. An example list of OFFICIAL classified information
    - Day-to-day business management and support, including strategy documents, corporate communications, records of routine meetings, general email communication.

- Personal and customer information, including recruitment, Adelphi and PDR records, Freedom of Information (FOI) requests.
- Commercial information, including supplier management information, internal communications relating to contracts.
- Non-sensitive policies including formulations and proposals; submissions and advice to Ministers.
- General staff records.
- Organisation level policies and procedures which are available to the both TCS and DBS staff.

c) There is no requirement to explicitly mark OFFICIAL information and any information which does not have a classification marking shall be treated as OFFICIAL information and shall be handled in accordance with the controls specific to OFFICIAL classification.

4.2 OFFICIAL SENSITIVE Classification

4.2.1 Adding the SENSITIVE caveat to the OFFICIAL classification is a sign that additional controls are required when handling this type of information/data .This is not a classification in its own rights and using the SENSITIVE handling caveat does not constitute a higher security classification than OFFICIAL. This should be used by exception in limited circumstances and should have a clear and justifiable requirement to reinforce the need to know, the compromise or loss could have damaging consequences for an individual or group or cause significant reputational damage to the organisation.

4.2.2 An Example list of OFFICIAL-SENSITIVE classified information

a) Business management information, including organisational change, security risk assessments and detailed technical design information.
b) Criminality data including cautions, convictions and local intelligence.
c) DBS Barred list information (e.g. – POVA, List 99, POCA, Adult and Children) or Information matched to a barred decision.
d) Sensitive personal information, including medical issues, disciplinary action, internal investigation details, alleged misconduct and poor performance reviews, gender reassignments, transgender, high profile cases (i.e. - Celebrities, MPs, and media covered cases), witness protection etc.
e) Commercial information relating to contract negotiations, external communications and procurement tender exercises.
f) Sensitive or contentious policies; sensitive ministerial correspondence, submissions.

The above list is not exhaustive, but should provide a clear indication of the type of data handled within TCS/DBS that requires the SENSITIVE handling caveat.

4.2.3 The compromise of OFFICIAL-SENSITIVE information or material would be likely to have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the “OFFICIAL" classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the “need to know". In such cases where there is a clear and justifiable requirement to reinforce the “need to know", assets should be conspicuously marked: “OFFICIAL–SENSITIVE’

4.2.4 Assigning the SENSITIVE caveat to an information asset determines the additional protective security controls required. It is therefore very important

that staff “valuing” information assets apply the caveat carefully and in doing so the following should be considered

a) The incorrect attribution of a caveat means that overly protective security controls are used; this is not only potentially expensive and time-consuming, but also inhibits the effective use of information or other assets and disrupts business unnecessarily
b) Not applying a caveat when required means that the material is put at risk as appropriate protective security controls will not be applied.

5.0 Responsibility of Information Classification

5.1 An asset must be classified and protected to cater for the most sensitive component of it, e.g. if a document contains elements of OFFICIAL and OFFICIAL-SENSITIVE information, the overall classification of the document will be “OFFICIAL-SENSITIVE.

5.2 By default all TCS/DBS information is classified as OFFICIAL. Where the OFFICIAL-SENSITIVE caveat is to be considered, it is for the originator or the information owner to determine the classification and the control of its initial distribution. Once the initial classification has been set, the following points must be observed in the management of the classification:

a) Only the originator/owner may change the information’s classification (within the parameters set out in this policy.)
b) The originator/owner retains the prerogative to remove any particularly sensitive elements to facilitate a wider dissemination of the information. Equally, they may also decline a request to do so in the interests of confidentiality.
c) Where the information is classified as OFFICIAL-SENSITIVE, the originator/owner is obligated to ensure handling instructions are applied in accordance with this policy and to detail with the handling instructions if at a later date the classification could be downgraded to OFFICIAL
d) If there is a requirement to remove the OFFICIAL-SENSITIVE caveat to enable a wider distribution of the information, then the authorisation of the originator/owner must be sought to clear its use.

5.3 Information Data Owners are responsible for identifying any sensitive Information within the OFFICIAL-SENSITIVE category and for putting in place appropriate business processes to ensure that it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements

5.4 All personal Information irrespective of its classification is subject to the provisions of the UK Data Protection Act 1998, in particular Principle 7 of that Act which states:

e) Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

.

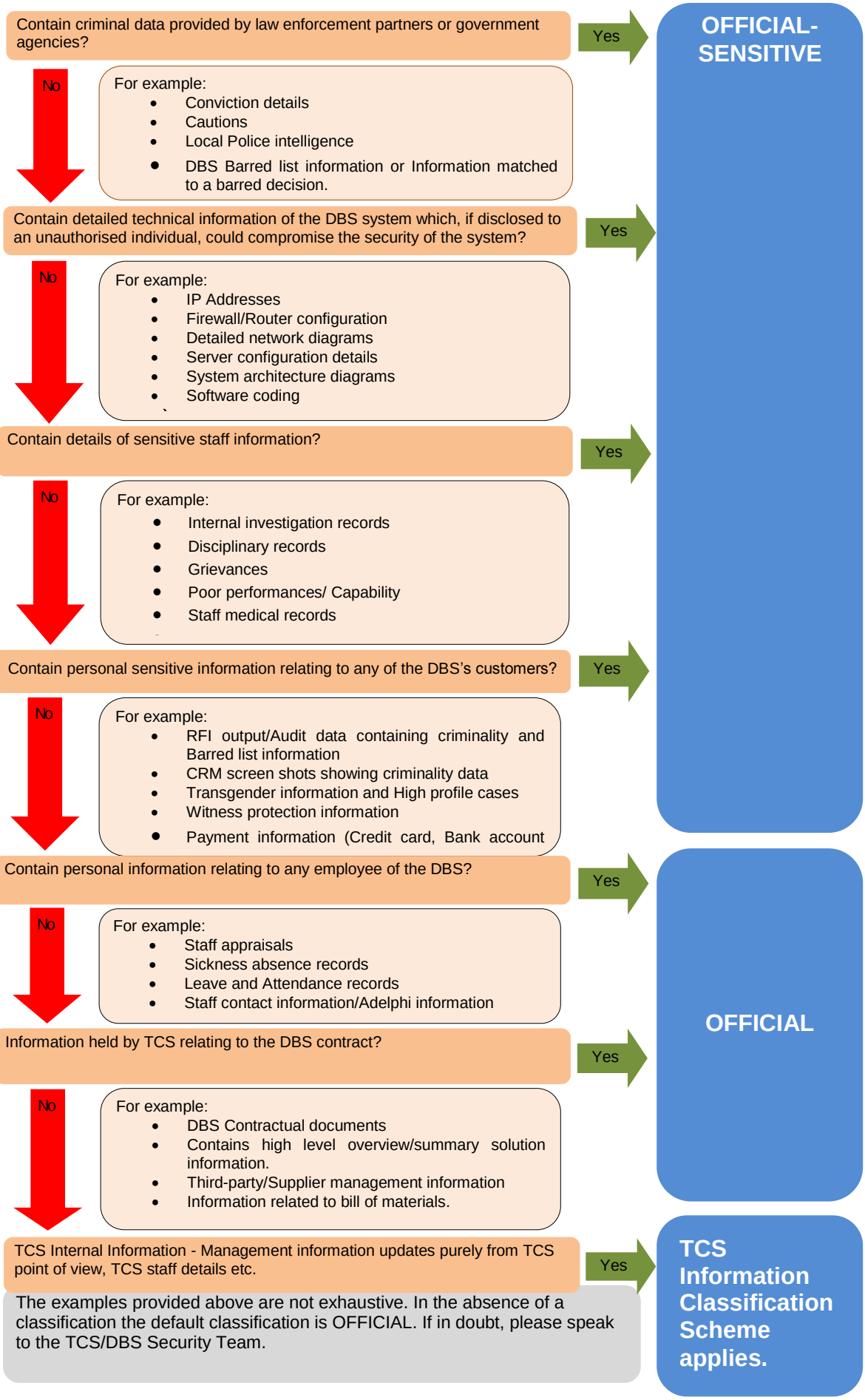
5.5 ALL HMG information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack

5.6 TCS/DBS staff must understand that they are personally responsible for securely handling any information that is entrusted to them in line with local business processes.

5.7 All information that is classified as OFFICIAL-SENSITIVE must be marked in the document or media in accordance with the Information Media Labelling and Handling Requirements stated below

5.8 . TCS/DBS Staff will be accountable and responsible for all the information they create or have custody of. All staff shall ensure that the information receives the appropriate protection and is only shared with those who have a legitimate need to know. If in doubt, they should seek advice from their Line Manager and/or TCS/DBS Security team

6.0 Information Classification Tree



7.0 Information Media Labelling and Handling Requirements

The labelling and subsequent handling requirement for OFFICIAL and OFFICIAL-SENSITIVE TCS/DBS information assets are defined in the below sections. The requirements are not limited to marking and distributing documents, but also refer to the correct handling of electronic media, faxes, telephone calls, postal mail etc.. DBS Security Aspects Letter (SAL) shall be followed in entirety for all Information Handling requirements.

7.1 Document Labelling & Handling (i.e. hard copy, paper documentation.)

	OFFICIAL or "No Marking on the information"	**OFFICIAL-SENSITIVE**
Document labelling	There is no requirement to mark OFFICIAL information. All pages must be marked "page x of y" (e.g. Page 1 of 10).	Marked top and bottom with the words: OFFICIAL-SENSITIVE All pages must be marked "page x of y" (e.g. page 1 of 10).
Document Distribution (internal post includes delivery between 1-TBS and Shannon Court)	Sealed envelope. DBS/TCS recipient's name and department.	Sealed envelope marked OFFICIAL-SENSITIVE for the attention of the "Addressee Only."
Document Distribution (External)	Ordinary sealed envelope marked for the attention of the addressee only. The envelope should be addressed to a specific individual (by name or appointment.) The sender's details should be provided with a return address for undelivered items.	**Sending OFFICIAL-SENSITIVE by post** Use a double-cover with the information being placed in the inner envelope only. The outer envelope must never be marked with the caveat and a return address must be included. Use first or second class post. Consider a register Royal Mail Service or reputable commercial courier's 'track and trace' service if required. Barring post is to be sent by Royal Mail Recorded or Special delivery..
Faxing	OFFICIAL information may be sent via FAX. Use fax templates/cover sheets providing contact details.	Mark fax as: OFFICIAL - SENSITIVE Use fax templates/cover sheets providing contact details. Consider not using one touch

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
		dialling in case the number has been changed or corrupted. Consider only sending once the intended recipient has been phoned and has confirmed that they are able to collect the fax immediately. Ask for confirmation of receipt from the recipient.
Storing paper in the office	To be kept in locked storage when unattended.	To be kept in locked storage when unattended. Consider using appropriate physical security equipment/furniture.
Destruction of paper	To be disposed in confidential waste bins or shredded. If away from base office, retain the material and dispose of securely on return to office.	To be disposed in confidential waste bins or shredded. If away from base office, retain the material and dispose of securely on return to office.
Photocopiers & Scanners	Only photocopy or scan information when there is a business requirement to do so.	Only photocopy or scan information when there is a business requirement to do so.

7.2 Portable Media Labelling & Handling (i.e. USB memory sticks, CDs)

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
Portable media labelling	There is no requirement to mark the media containing OFFICIAL information. Use of portable media should be minimised. Other approved information exchange mechanisms should be used where available. Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement.	The media (and any casing) should be marked with the words: OFFICIAL-SENSITIVE Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement.

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
Internal distribution of portable media	Portable media should be handed in person to intended recipient. Consider data encryption using a FIPS 140-2 certified product.	Portable media should be handed in person to intended recipient. Must be encrypted, consider CPA foundation grade encryption to protect the content, particularly where it is outside the TCS/DBS's physical control.
External distribution of portable media	Data must be encrypted using a FIPS 140-2 certified product. Ordinary sealed envelope marked for the attention of the addressee only. The envelope should be addressed to a specific individual (by name or appointment.) The sender's details must be provided with a return address for undelivered items. Consider tamper-proof envelopes. Use a trusted courier or Recorded Delivery.	Data must be encrypted using a CPA foundation grade encryption product. Ordinary sealed envelope marked for the attention of the addressee only. The envelope should be addressed to a specific individual (by name or appointment.) The sender's details must be provided with a return address for undelivered items. Consider tamper-proof envelopes. Use double envelope. Use a trusted courier or Recorded Delivery.
Removal for re-use and/or destruction of data from Hard drives / portable media	Dispose of with care using approved commercial disposal products to make reconstitution unlikely. Destroy removable media/hard drives when no longer needed either through degaussing or use of approved software. Physical drives/media then disposed of through confidential waste bin for plastics/hard drives.	Dispose of with care using IS5 disposal products to make reconstitution unlikely. Destroy removable media/hard drives when no longer needed either through degaussing or use of approved software. Physical drives/media then disposed of through confidential waste bin for plastics/hard drives. Destruction activity must finish with submission of IS5 certificate.

7.3 Email

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
Emailed within GSi network	Ensure accuracy with email addressing. There is no requirement to label OFFICIAL information.	**Handling OFFICIAL-SENSITIVE emails** When sending OFFICIAL-SENSITIVE information via email, you must mark the email with this caveat. Specifically, the caveat must be clearly displayed in capitals within the subject box at the beginning of the title and at the top of the email text in capitals. Handling instructions must also be provided. .
Emailed within TCS Corporate network	Should only be sent to individuals approved to work on the DBS contract who met the pre-employment check criteria for the DBS programme. Must be sent only to relevant individuals with need to know.	Material classified as OFFICIAL – SENSITIVE must not be emailed within the TCS corporate network without using a CPA foundation grade encryption product.
Email from GSi network to addresses outside of the GSi / PNN / CJX/CJSM network (i.e. across internet.)	Routine information can be shared or emailed with external partners/citizens subject to internal procedures and policies. As with current arrangements, you must ensure that personal information in transit is protected and encrypted where there are confidentiality requirements to ensure compliance with Data Protection Act 1998.	Material classified as OFFICIAL – SENSITIVE must not be emailed outside of the GSi network without using a CPA foundation grade encryption product.
Email from TCS network to addresses outside of TCS network. (i.e. across internet)	Routine information can be shared or emailed with external partners/citizens subject to internal procedures and policies. As with current arrangements, you must ensure that personal information in transit is protected and encrypted where there are	Material classified as OFFICIAL –SENSITIVE must not be emailed over the internet without using a CPA foundation grade encryption product.

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
	confidentiality requirements to ensure compliance with Data Protection Act 1998.	

7.4 Storing of all media types

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
Storing media in the office	All personal data within the OFFICIAL tier whether Citizen or Staff data must be kept in locked storage when not in use or when outside of normal office hours.	All personal data within the OFFICIAL –SENSITIVE tier whether Citizen or Staff data must be kept in locked storage when not in use or when outside of normal office hours. Consider use of appropriate physical security equipment/furniture.
Storing data on the system file shares	Data must be stored and accessible based on need to know principle.	Data must be stored and accessible based on need to know principle. Use systems with access permissions implemented on them. In addition to mandatory access control lists, consider applying password protection on files or folder structure. Data must be stored on a secure accredited network.

7.5 Communications

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
Telephones/ Telephone conferencing facility	May be discussed over a public telephone network.	Discussions of sensitive nature over a public network to be kept to a minimum. Be conscious of eaves dropping or being over heard. Avoid having sensitive conversations in public places. Do not leave sensitive information on voicemail.
Registered Video Conferencing	May be discussed over a Video conferencing system.	Discussions of sensitive nature over a video conferencing to be kept to a minimum.

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
Facility		Consider audience on need to know principle. Consider alternative mechanism for sharing the more sensitive information.

7.6 Offshore information sharing

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
Recipient	Should only be sent to individuals approved to work on the DBS contract who met the pre-employment (equivalence process) check criteria for the DBS programme. Must be sent only to relevant individuals with need to know.	Must not be used.
Telephone / Telephone conferencing facility	May be discussed over a public telephone network. Consider discussion only when the other party is available within TCS premises.	Must not be used.
Registered Video Conferencing Facility	May be discussed over a registered Video conferencing system. Consider discussion only when the other party is available within TCS premises.	Must not be used.
Email	Must only use TCS email. Follow TCS Email guidelines.	Must not be used.
Fax	Use fax templates/cover sheets providing contact details.	Must not be used.
Personal transfer	OFFICIAL information may be taken to offshore with valid business requirement to deliver services from TCS offshore location where transfer is within the DBS contract. You must ensure that no UK Citizen information is taken	Must not be transferred.

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
	offshore.	
Storing data on the system file shares for offshore access	OFFICIAL information should only be stored offshore with valid business requirement. Data must be stored and accessible based on need to know principle. Use systems with access permissions implemented on them. In addition to mandatory access control lists, consider applying password protection on files or folder structure. Data must only be stored on approved TCS Corporate Infrastructure or the TCS offshore network provisioned for the DBS contract. You must ensure that no UK Citizen information is taken offshore.	Must not be transferred.
Courier	OFFICIAL information may be sent to offshore with valid business requirement. Ordinary sealed envelope marked for the attention of the addressee only. The envelope should be addressed to a specific individual (by name or appointment.) The sender's details must be provided with a return address for undelivered items. Consider tamper-proof envelopes. Use a trusted courier or Recorded Delivery. You must ensure that no UK Citizen information is taken	Must not be transferred.

	OFFICIAL or "No Marking on the information"	OFFICIAL-SENSITIVE
	offshore.	
Use of mobile media equipment (i.e. – laptops, USB/external Hard drives)	OFFICIAL information may be used offshore with valid business requirement on an approved media/Equipment. Do not leave mobile equipment or media unattended. Avoid using them in public places. You must ensure that no UK Citizen information is taken offshore. A list must be maintained for all media or equipment used offshore in accordance with the TCS Asset Management procedure.	Must not be transferred.
Web based meeting channels (i.e – Goto meeting, webex)	OFFICIAL information may be discussed with valid business requirement. You must ensure that no UK Citizen information is discussed or shown offshore. Consider discussion only when the other party is available within TCS premises.	Must not be discussed

8.0 Breach of Policy

a) Any unauthorised reduction or removal of the classification of a document in order to avoid handling instructions will constitute a direct breach of this policy.

b) A failure to protect, information appropriately has the potential to undermine the work of the TCS/DBS. Such failures will constitute a breach of this policy. All such breaches will be considered as security incident and will be dealt with respect to the TCS/DBS Information Security Handling Policy

9.0 Exceptions

There are no exceptions to this policy