CGS-CIMB GROUP
DATA GOVERNANCE POLICY

SECTION : TABLE OF CONTENTS
SUB-SECTION :

Abbreviation	**Definition / Descriptions**
Branch Office	A Branch Office refers to an overseas branch/office operating outside Singapore.
CGS-CIMB Group Employee	Employees include CGS-CIMB Group's permanent staff, temporary staff, contract staff, seconded staff, interns and such other staff as determined by Group Compliance to be subjected to this Policy.
CGS-CIMB Group or the Group	CGS-CIMB and its group of companies as per the organisation chart maintained by the Company Secretarial from time to time
Enforcement Agency	Enforcement Agency is a government agency responsible for the enforcement of the laws.
Information	For the purpose of this Policy, Information is defined as any information, documents, data and records that are known publicly and otherwise, collected/ owned by/ related to CGS-CIMB Group in the course of the business, regardless of their location in the form of softcopy and hardcopy.
Information Provider	Any person or entity that is responsible, in whole or in part for providing the Information to the Information Requester.
Information Provider's Designated Person	Head of Division/Department or his/her delegate is to release and/or approve the request to release or provide the Information requested.
Information Requester	Any person or entity that requests, in whole or in part of Information for a specific reason/purpose.
Information Requester's Designated Person	Head of Division/Department or his/her delegate is to request and/or approve the request to request for Information.

CGS-CIMB GROUP DATA GOVERNANCE POLICY	
SECTION SUB-SECTION	: ABBREVIATION AND DEFINITION/ DESCRIPTIONS :

Abbreviation	**Definition / Descriptions**
Subsidiary	Subsidiary is a company where CGS-CIMB Group holds more than a total of 50% of the company's equity either directly or through the companies within the group.
Sharing of Information	Sharing of Information refers to sharing of any Information between entities within CGS-CIMB Group in different jurisdictions. This Policy & Procedures is not applicable to CGS-CIMB Group entities where both Information Requestor and Information Provider are situated in the same country.

CGS-CIMB GROUP DATA GOVERNANCE POLICY		
SECTION 1	:	INTRODUCTION
SUB-SECTION	:	

1.1 Introduction

Sharing of Information within circumstances which are permitted by the laws and regulations are the key of delivering better and more efficient services for the CGS-CIMB Group and its branch offices and subsidiaries (herein referred to as "CGS-CIMB Group"). Sharing of Information in an appropriate manner is a vital element for CGS-CIMB Group's Management and Board of Directors to oversee and establish sound corporate governance across CGS-CIMB Group.

Information is an asset; every employee and department within CGS-CIMB Group uses Information on a daily basis to perform their role. The source of the Information has to be managed and used appropriately to ensure CGS-CIMB Group meets its responsibilities and statutory obligations.

Appropriate handling of sharing of Information will safeguard CGS-CIMB Group from the following:-

i. the risk of non-compliance to the law and potential enforcement action by regulators;
ii. any potential exposure to legal risk arising from unauthorised disclosure bound by non-disclosure agreement; and
iii. any reputational risk caused by inappropriate information sharing.

1.2 Objective

The objective of this Policy is to establish a proper framework within which sharing of Information is permissible within the CGS-CIMB Group.

Compliance by CGS-CIMB Group's Employees with this Policy is mandatory. Any breach/violation of this Policy is to be escalated to Group Compliance immediately. Appropriate disciplinary action will be taken which may include, reprimand or warning, up to and including, termination of employment.

1.3 Conflict of Guidelines

Where there is a conflict or discrepancy between this Policy and the local requirements, the more stringent standard is to be applied. In the event where the entity/subsidiary is unable to adopt the more stringent requirements in this Policy, the entity/subsidiary is required to escalate the matter to Head of Division and Group Compliance in writing to seek advice and, where applicable, approval from the Board of Directors of the relevant entity.

1.4 Maintenance

This Policy is subject to review at least once in every two (2) years or at such other period as Group Compliance may deem necessary, whichever is earlier. Notwithstanding this, the Board of Directors of CGS-CIMB Group may request for such review from time to time.

1.5 Circulation

A copy of this Policy is made available to all CGS-CIMB Group Employees via Confluence. Amendments and updates are to be posted on Confluence by Group Compliance as and when there are changes in the applicable laws, regulations, guidelines and policies.

Each employee is required to read, understand and comply with this Policy and any amendments and updates hereto. Violations of this Policy may be grounds for disciplinary action including but not limited to termination of employment.

All employees and agents of the Group must strictly comply with the Policy. Employees include permanent staff, contract staff, management trainee, salaried dealer representative, seconded staff and such other employees as determined to be covered under the Policy.

1.6 Proprietary Rights

This Policy is the property of Group Compliance and is strictly for internal use. No parts of this Policy or its contents are to be revealed to outside parties or reproduced in any form without the prior consent of the Group Head Compliance.

1.7 Relevant legislation, regulations and policies

This document must be read in conjunction with relevant regulations and guidelines, including but not limited to the relevant client confidential information and personal data protection laws in each country and the following:

i. CGS-CIMB Group Personal Data Protection Policy & Procedures;
ii. CGS-CIMB Group Conflict Management & Chinese Wall Policies & Procedures ;
iii. CGS-CIMB Group Communications Policy;
iv. CGS-CIMB Group Data Management Policy which is part of CGS-CIMB Group Information Technology Policy;

[End of Section]

2.0 Sharing of Information

There are circumstances where sharing of Information is required. CGS-CIMB Group Employees must determine whether Information is shared in accordance with the policies, laws and regulations.

Prior to sharing of any Information in relation to CGS-CIMB Group, CGS-CIMB Group Employees must also determine whether there is a clear and legitimate purpose for sharing such Information and whether the Information required contains any confidential data.

CGS-CIMB Group Employees must be aware that there are practices that must be avoided when sharing Information.

The following practices could potentially lead to legal and/or regulatory action:-

i. unauthorized disclosures/breach of secrecy obligations;
ii. mislead individuals about the intention of sharing their Information;
iii. share excessive or irrelevant Information;
iv. not taking reasonable steps to ensure that Information is accurate and up to date before sharing it;
v. use incompatible information systems to share Information resulting in the loss, corruption or degradation of the data.

[End of Section]

3.0 Types of Information

There are two (2) categories of Information involved in CGS-CIMB Group's daily operations, namely Public Information and Non-Public Information.

The administration of Information must be carried out with the consideration of risk management.

Information can be in the form of softcopy or hardcopy, both owned by CGS-CIMB Group and its customers.

3.1 Public Information

Public Information refers to Information that is known by the public. Examples of Public Information include but are not limited to:-

i. Public filings with regulators;
ii. Issuance of press release by the company;
iii. Disclosure of information in financial media; and
iv. Information contained in proxy statements and prospectuses.

Sharing of Public Information by CGS-CIMB Group Employees is not prohibited. However, CGS-CIMB Group Employee must be cautious in the event the Public Information is related to customer's financial affairs and such Information has been provided to CGS-CIMB Group by the customer in relation to investment banking activities with CGS-CIMB Group. Under such circumstances, this Information must be treated as Non-Public Information which can only be disclosed in accordance with the laws, regulations and policies requirements.

3.2 Non-Public Information

Non-Public Information is the type of Information that is unknown to the public and encompasses the following:

3.2.1 <u>CGS-CIMB Group's Client Confidential Information</u>
Information subject to CGS-CIMB Group Client Confidential Information refers to

any information connected to the relationship between CGS-CIMB Group and its customers, such as customer data, transactions and financial affairs. These types of Information must be treated as confidential Information and CGS-CIMB Group Employees are obligated to take every precaution to protect the confidentiality of such Information.

Sharing of CGS-CIMB Group's Client Confidential Information must be made and/or submitted in writing with clear purpose.

It is the responsibility of Information Requester and Information Provider to ensure that the sharing of CGS-CIMB Group's Client Confidential Information can only be done as long as the following conditions are met:

i. Compliance with policies, laws and/or regulations;
ii. Customer's written consent to disclosure has been obtained or in case where no consent has been given, the exemptions under the relevant laws permit such disclosure;
iii. Compliance with the terms of the Non-Disclosure Agreement executed with customer (where applicable); and

3.2.2 Information Relating to CGS-CIMB Group Internal Undertakings

This is referring to Information owned by CGS-CIMB Group internally, such as Policies, Procedures, Standard Operating Instructions, Manuals, Minutes of Meetings, as well as internal Financial and Personnel Information.

CGS-CIMB Group Internal Undertakings Information includes but is not limited to:-

i. Information relating to CGS-CIMB Group's Corporate Strategy and Governance;
ii. Information relating to CGS-CIMB Group's Business Units, such as Fund Management and Investment Banking; and
iii. Information relating to CGS-CIMB Group's Support Functions including but not limited to Finance, Human Resources, Compliance, Legal, Information and Operations, Risk and Marketing and Communications.

While sharing of Non-Public Information relating to CGS-CIMB Group Internal Undertakings is not prohibited, however, the sharing party must ensure the confidentiality of the Information shared is safeguarded and/or protected, not be shared with any person outside the CGS-CIMB Group and request is approved by the Information Requester's Designated Person.

3.2.3 Information Relating to Regulator's Audit, Inspection and Review

Such information includes all reports issued by the regulator in connection to the outcome of any audit, inspection and/or review conducted in connection to CGS-CIMB Group.

Sharing of Non-Public Information relating to CGS-CIMB Group regulator's Audit, Inspection and/or Review is only to be permitted provided the respective regulator's approval (regulator that conducted the Audit, Inspection and/or Review) has been obtained where is required by local regulations.

3.3 DATA CLASSIFICATION POLICY

Business Units are responsible to ensure that the Data Classification must be performed on the data owned.

3.3.1 Data Classification Categories

No	Category	Description
1	Highly Confidential	Unauthorised disclosure of highly confidential data could result in significant adverse impact, reputational risks or penalties to the Group. It is used for highly sensitive information whose access is restricted to selected, authorised employees and must be protected at all times. Security at this level is the highest. Some examples of Highly Confidential data include: (a) Impending mergers or acquisitions; (b) Investment strategies; (c) Plans or designs; and (d) Root passwords of critical systems operating systems and database.

No	Category	Description
2	Confidential	Confidential information is protected by statutes, regulations, or contractual agreements. This information, if made public or even shared among the Group, could seriously impede the Group's operations and is considered critical to its ongoing operations. Such information must not be copied or removed from the Group's operational control without specific authority. Security at this level is very high. Some examples of confidential data include: (a) Financial information; (b) Business plans; (c) Customer information; (d) Staff data including payroll; and (e) Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.
3	Proprietary / Internal Use Only	This type of information is restricted to members of the Group/Division/Department only who have a legitimate purpose for accessing such data and must be guarded due to proprietary, ethical, or privacy considerations. However can be released to third party if the document is meant to be released to outside Group. It must be protected from unauthorised access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Security at this level is high. Some examples of proprietary/internal use information include: (a) User guidelines; (b) Operational work routines; (c) Project plans and designs; (d) Specifications that define the way in which the Group operates; (e) Policies & procedures; (f) Internal memos and emails;

No	Category	Description
		(g) Internal project reports; (h) Internal telephone books and directories; and (i) Organisation Chart
4	Public	Public data is information open to the general public, where the security level is minimal. It is defined as information with no existing local, national or international legal restrictions on access or usage.

3.3.2 Highly Confidential Data

(a) The recipients of Highly Confidential Data have an obligation not to reveal the contents to another individual unless that person has a valid need to know the information.

(b) Departmental procedures must be in place to ensure that all individuals who have access to Highly Confidential information are aware of the sensitivity of the information to which they have access, understand their responsibilities to protect that information appropriately, and acknowledge their understanding and intent to comply with this Policy.

(c) Below are the standard policies applied for Highly Confidential information, but not limited to the following table:

No	Standard Policy	Statements
1	Transmission by post, and email standards	(a) For mail between departments, must ensure sealed inter-office envelope marked as 'Highly Confidential' and to notify the recipient in advance; (b) For mail (and/or email) to vendors or third parties, marked as "Strictly Private and Highly Confidential", "Private and Highly Confidential" OR "Highly Confidential" is required. Traceable delivery, e.g., recorded delivery or special delivery is compulsory; and

No	Standard Policy	Statements
		(c) Use of email for Highly Confidential Data is strongly discouraged, unless encrypted.
2	Copying standards	Photocopying can only be done with approval from the owner of the information. If a digital copier is used, the cache needs to be erased after use.
3	Access control standards	(a) Content modification is restricted to authorised individuals as needed; and (b) Authentication and authorisation are required for access.
4	Storage standards	Refer to CGS-CIMB Group Data Management Policy which is part of CGS-CIMB Group Information Technology Policy (For Data identification, architecture and media control).
5	Destruction standards	(a) Approval must be sought from HOD of the respective BUs to destroy this type of data; (b) No contracts with external waste contractors are allowed unless it is Group approved and authorised vendor; (c) Paper recycling is not allowed; and (d) Destruction of all data is by any method which makes record reconstruction impossible.
6	Physical security standards	(a) Do not leave data unattended. Sign-off or power-off workstations or terminals when workstation is not in use or leaving work area; and (b) Highly Confidential information must be locked when left in an unattended room.

3.3.3 Confidential Data

(a) Confidential data may be disclosed to individuals on a "need-to-know" basis only.

(b) Below are the standard policies applied for Confidential information, but not limited to:

No	Standard policy	Statements
1	Transmission by post and email standards	(a) For mail between departments must ensure sealed inter-office envelope marked as 'Confidential'; (b) For mail (and/or email) to vendors or third parties, marked as "Strictly Private and Confidential", "Private and Confidential" OR "Confidential" is required. Traceable delivery, e.g., recorded delivery or special delivery is preferred; and (c) Use of email for Confidential Data requires storage in a secured manner.
2	Copying standards	Photocopying is to be minimised, only when necessary and approved by the data/information owner. If a digital copier is used, the cache needs to be erased after use.
3	Access control standards	(a) Content modification restricted to authorised individuals as needed; and (b) Authentication and authorisation are required for access.

Storage Standards, Destruction Standards as well as Physical Security Standards are similar to the policies as set for Highly Confidential classification.

3.3.4 Proprietary/Internal Use Data

Below are the standard policies applied for proprietary/internal use information, but not limited to:

No	Standard policy	Statements
1	Transmission by post, fax and email standards	(a) No special handling is required for post and email; (b) Fax location is not to be located in an area accessible to the general public; and (c) For email of internal use, marked as "Proprietary/Internal Use Only" is encouraged.
2	Copying standards	No special precautions required.
3	Access control standards	(a) Generally available to all authorised users on a "need to know" basis; and (b) Content modification is restricted to authorised individuals as needed.
4	Storage standards	Reasonable precautions to prevent access by nonemployees.
5	Destruction standards	(a) Reasonable precautions to prevent inadvertent disclosure; and (b) Paper recycling which contains internal information is not permitted.
6	Physical security standards	(a) Do not leave data unattended. Sign-off or power-off work stations or terminals when workstation is not in use or leaving workstation area; and (b) Information must be locked when left in an unattended room.

3.3.5 Public Data

(a) Disclosure of Public Data must not violate any pre-existing signed non-disclosure agreements.
(b) The integrity of Public Data should be protected, and the appropriate department or unit must authorise replication or copying of the data in order to ensure it remains accurate over time.

3.4 CUSTOMER DATA CLASSIFICATION

Customer data is classified as "Confidential". Customer herein refers to individuals and non-individuals (legal persons, including shareholders, directors, guarantors and persons authorized by non-individual customers).

To aid customer data sharing and data protection measures, this Policy further elaborates the definition of customer data categories and classes.

Three (3) classes of customer data defined, namely Class-1, Class-2 and Class-3. For non-individuals the information includes shareholders, directors, guarantors and persons authorized by non- individual customers.

(a) Class-1 Customer Data

Class-1 customer data consists of personally identifiable information (PII) which relates directly or indirectly to a customer, and can be identified or identifiable from that information. It also means any attributes that can be linked to or can identify a specific individual through association or inference. Examples of Class-1 customer data are:

i. Customer Name;
ii. Postal Address;
iii. Email Address;
iv. Phone Number;
v. Account Number and;
vi. Identification Number

Class-1 customer data requires the highest security protection during transmission and usage of customers' data as unauthorised access or misuse of such data places the survival of the business at risk. Refer to Data Encryption of Group Information Security Policy and Data Loss Prevention of Group IT General Control Policy. Sharing of Class-1 customer data requires concrete justification by Data or Information Users and must provide assurance to avoid any unauthorised or misused to the customers' data.

(b) Class-2 Customer Data

Class-2 customer data are information that is not specific to a particular customer, whereby upon deeper investigation or search does not directly identify the owner of the information. Class-2 customer data is less confidential compared to Class-1 customer data. Examples of Class-2 customer data are:

i. Citizenship;
ii. Constitution;
iii. Gender;
iv. Marital status and;
v. Profession.

(c) Class-3 Customer Data

Class-3 customer data are general information such as hobbies, interests, lifestyle preferences or product information tagged to the customer data.

[End of Section]

4.0 Information Retention

Information retention process and/or requirements are to be decided depending on the purpose and usage of the Information. Information provided may not be required to be kept indefinitely or longer than needed with regard to the intended purposes.

In addition, the information retention must also be in accordance to regulatory and CGS-CIMB Group policy requirements. Where there is a conflict between the regulatory and CGS-CIMB Group policy requirements, the more stringent requirements are to be adopted to the extent that they are permitted by the respective country's law and regulations.

[End of Section]