

Information Protection Policy
The Global Credit Data Consortium

Version 1.5

Revised July 2018

Revised November 2020

Information Classification: PUBLIC

Document Control

Organisation	Global Credit Data
Title	Information Protection Policy
Author	Philip Winckle – Richard Crecel
Filename	Global Credit Data Information Protection Policy v1.4.docx
Owner	Executive Director
Subject	IT Policy
Information Classification	PUBLIC
Review date	July 2018 – November 2020 – (next review: 2022)

Revision History

Revision Date	Version Number	Revised By	Description of Revision
25 Oct 2013	1.0	PW	First draft
16 Dec 2013	1.1	PW	Added enforcement section
28 Feb 2015	1.2	PW	Name change only from PECDC to GCD
7 Nov 2017	1.3	PW	Increased security for level 6 information
July 2018	1.4	PW	Addition of information class
November 2020	1.5	RC	Removed: <ul style="list-style-type: none"> - restriction “... for executives ...” to include third party associates - “(...) data are priceless (...)” Updated: <ul style="list-style-type: none"> - Classification Levels: “Restricted” category is applicable to information distributed via third-party, if any - “Enforcement of Policy” + obligation of annual training for GCD executives

Document Approvals

This document requires the following approvals:

Approval Authority	Name	Approval
Executive Director	Richard Crecel	Nov 2020
Board Admin Standing Subcommittee	Theo van Drunen	
Board of Directors	Theo van Drunen	15 Dec 2020 Board Meeting

Document Distribution

This document will be distributed to:

Organisation	Persons (if not all)
Members via website	all
Potential members	all
Executives	all
Data Agents	all
Service Providers	On need to know basis

Contents

Background and purpose: 4

Policy Statement: 4

Scope: 4

Definition:..... 4

Risks:..... 4

Review and Revision:..... 5

References:..... 5

Classification of Information: 5

Contracts with executives and consultants: 8

End of Document..... 8

Global Credit Data Information Protection Policy

Background and purpose:

The Global Credit Data Consortium is registered in Netherlands as an Association and is referred to herein as “Global Credit Data” or “GCD”.

GCD’s mission requires it to collect, aggregate and share credit data which is provided by its member banks. This data varies from borrower level information through to aggregated statistics and even bank model parameters from time to time. All of this data is confidential for the following reasons: viewing the data submitted by a single bank could give information about a bank’s portfolio or practices; viewing the database as a whole is only allowed for member banks on a give to get basis.

The data, information, reports, etc. which GCD holds are of value to the member banks and should be available to members on an ongoing basis.

This policy details the basic requirements and responsibilities for the proper management of information assets at GCD. The policy specifies the means of information handling and transfer within the Association.

Policy Statement:

GCD will ensure the protection of all information assets within its custody of the association.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

Scope:

This Information Protection Policy applies to all the systems, people and business processes that make up GCD's information systems. This includes all Committees, Working Groups, Executives, Employees, contractual third parties and agents of GCD who have access to Information Systems or information used for GCD’s purposes.

For the avoidance of doubt, this policy does not set out the rules of give to get, critical mass and other data sharing or publication regulations, which are governed by the Articles of Association and the Data Pool Regulations.

Definition:

This policy should be applied whenever Business Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using email or other electronic means.
- Stored audio or video in any format, including web based presentations.
- Speech.

Risks:

GCD recognises that there are risks associated with users accessing and handling information in order to conduct official business of the association.

This policy aims to mitigate the following risks:

- Data submitted by a member bank becoming available to a person or organisation not authorised to have it
- All or part of a database becoming available to a party who has not performed the obligations required to receive it (give to get)

- Data coming into the public domain without GCD's knowledge or control and being used to discredit the reputation or business of GCD or a member bank
- Data being lost or corrupted which would reduce GCD's ability to correctly process and return it to member banks
- Information, reports, etc. becoming available to parties who do not have the right to receive them
- Information, reports, research, minutes, etc. being lost or corrupted and therefore no longer available to GCD or its member banks.

Non-compliance with this policy could have a significant effect on the efficient operation of the association and may result in financial or reputational loss to GCD or to its member banks and an inability to provide necessary services to our members.

Review and Revision:

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 24 months.

Policy review will be undertaken by the Executive Director

References:

The following documents are directly relevant to this policy:

- Global Credit Data Articles of Association
- Global Credit Data Data Pool Regulations
- Data Agent Services Agreement with Capgemini
- Service contracts with Executives and Service Providers
- The Information Security Procedures

Classification of Information:

On creation, all information must be assessed and classified by the responsible party according to the content. The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification. GCD requires information assets to be protectively marked into one of 7 classifications. Where the information could fit more than one classification then it is to be classified into the higher classification. The way the document is handled, published, moved and stored will be dependent on this scheme.

The classes are:

	Content	Example (not limited list)	Access to information/data	Storage	Transmission
1 Unclassified	Information which does not need to be protected or kept secret in any way.	Documents publicly downloaded from regulatory bodies.	World	Stored or backed up on centralised facilities.	Via email or other web based transmission services.
2 Public	Information which could be available to the general public but which GCD wants to protect to ensure that it is available in future in an uncorrupted way.	Annual LGD LC Report. Recovery Rates dashboards.	World GCD Copyright	Stored or backed up on centralised facilities to allow regular backups to take place. Records management and	Via email or other web based transmission services. Public website.

				retention guidance will be followed so that it is clear how long data is to be kept.	
3 Restricted	All data, reports and information available only to GCD members but not to the general public.	<p>Reports produced for the General Meetings.</p> <p>Information directly distributed to GCD members, or to other users of GCD information; or distributed via a third party (e.g.: Financial information company collaborating with GCD to distribute risk metrics based on the pooled data).</p>	<p>All Members</p> <p>Executives</p> <p>Data Agents</p> <p>Consultants on case by case basis</p> <p>Approved academic researchers</p> <p>GCD Copyright</p>	<p>Stored or backed up on centralised facilities to allow regular backups to take place.</p> <p>Records management and retention guidance will be followed so that it is clear how long data is to be kept.</p>	<p>Via email or other web based transmission services.</p> <p>Member website.</p>
4 Confidential	All data, reports and information available to all members of a certain Data Pool or working group but not to all members of GCD. Example is a special report for a data pool.	A special report for a data pool e.g. Shipping.	<p>Selected Members</p> <p>Executives</p> <p>Data Agents</p> <p>Consultants on case by case basis</p> <p>Approved academic researchers</p> <p>GCD Copyright</p>	<p>Stored or backed up on centralised facilities to allow regular backups to take place.</p> <p>Records management and retention guidance will be followed so that it is clear how long data is to be kept.</p>	<p>Via email or other web based transmission services.</p> <p>Member website – restricted to Data Pool Members.</p>
5 Secret	All data and reports only available to certain members of GCD on a give to get basis. This data does not contain the name or identifying number of the submitting bank.	Aggregated and anonymised LGD data ready for return to members.	<p>Authorized Members</p> <p>Executives</p> <p>Data Agents</p> <p>Approved academic researchers</p> <p>GCD Copyright</p>	<p>Stored and processed in a secure environment, i.e either within a secure facility or if outside then only held in encrypted files using drive, volume or</p>	<p>Only via acceptable security settings, such as encrypted files and/or VPN setups, FTPS or HTTPS and end to end encrypted mail.</p> <p>GCD Data Portal.</p>

				folder encryption and strong passwords.	
6 Very Secret	Applies to reports and information as described in 5 where the name or identifying number of the submitting bank is contained or could be easily inferred.	Peer Comparison report.	Authorized Members Executives Data Agents To be treated especially carefully and should not be allowed to be viewed outside of the submitting member bank and the data agents or executives performing the processing. GCD Copyright	Information must be stored in a secure environment, i.e within a facility which is physically secure, with restricted access to named persons and where remote access is only allowed by secure VPN. It is not to be seen by third parties performing analysis.	Only via acceptable security settings, such as encrypted files and/or VPN setups, FTPS or HTTPS and end to end encrypted mail. GCD Data Portal.
7 Top Secret	Applies only to data where the name or identifying number of the submitting bank is contained or could be easily inferred.	LGD data submitted by a member bank containing that bank's code number or name.	Authorized Members Executives Data Agents To be treated especially carefully and should not be allowed to be viewed outside of the submitting member bank and the data agents or executives performing the processing. It is not to be seen by third parties performing analysis. GCD Copyright	Information must be stored in a secure environment, i.e within a facility which is physically secure, with restricted access to named persons and where remote access is only allowed by secure VPN.	Only via acceptable security settings such as VPN setups. GCD Data Portal.

GCD staff, executives and consultants should not be allowed to access information level 4 or above until the Executive Director is satisfied that they understand and agree to the responsibilities for the information that they will be handling. Consultants shall have in place

similar procedures to ensure that they approve all personnel who have access to such information.

Contracts with executives and consultants:

GCD shall ensure that contracts with executives and consultants have strong confidentiality clauses and clauses giving effect to this policy.

Enforcement of this policy:

GCD staff will receive annual training dedicated to raising awareness of this policy and consolidating the acquisition of appropriate professional skills.

Any material breach of this policy detected by GCD executives, or by third party associates, shall be escalated to the line manager who informs GCD's Executive Director who shall then consider taking the appropriate action, which may include bringing the breach to the attention of the Board of GCD.

The Board shall then consider taking appropriate action, which may include contractual sanctions, warnings or any other action. The Board shall also consider whether the breach is serious enough to warrant being reported to the members of GCD, usually via the GCD's Annual Report of Activities shared with the annual General Meeting of Members, as per GCD's Articles of Association, chapter 7, article 24.

End of Document