



IMRS Department
(Internal)

Data Privacy and Protection Policy

GWC-IMRS-DPL-01

	Name	Designation	Date	Signature
Process Owner	Marilyn Nicholas	Assistant Manager Customer Service, IMRS	September 30, 2017	
Verified By	Elangovan Rajah	Senior Manager QA & Security- Business Support	September 30, 2017	
	Ajit Nair	Senior Manager, Projects Freight Forwarding	September 30, 2017	
Approved By	Bobby George	Senior Director Freight Forwarding	September 30, 2017	

Table of Contents

1.0. Managing of Personal Information Data..... 4

2.0 Physical Security Measures..... 5

3.0 Technical Security Measures..... 6

A. RECORDS AND REFERENCES..... 6

B. REFERENCE MATERIAL AND EXTERNAL REFERENCES 7

C. REVISION HISTORY 7



Scope

This policy applies to all GWC employees, suppliers, customer and other interested party's personal information on data privacy and protection obtained by GWC which is relevant with the transactions it regularly carries out.

This policy is adopted in compliance with Qatar Law Number 13 of 2016 or the Personal Data Privacy Law on protecting personal data.

Objectives

- This policy is aimed to assist or aid GWC employees in classifying data to determine its need for protection.
- Serves as a guide or reference to ensure compliance of the company with the Data Privacy and Protection.
- To ensure that processing personal data establish policy and implement measures that guarantee the safety and security of customer's personal data under GWC's custody.

Responsibility

Designation	Responsibilities
GWC authorized employee	All authorized personnel of GWC organization regardless of the type of employment must comply with the terms set out in this policy.
Supervisor/Assistant Manager/Manager	To instruct all GWC employees to be aware of the data privacy and protection.
Director/Head of Department	To ensure conformance to this policy and compliance to the legal requirements.

Terms and Definition

Terms	Definition
Personal Information	Refers to as personally identifiable information that concerns, or can be related to an identifiable individual.
Privacy	The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information
Collection	The collection of personal information directly from the person and how information is brought together or recorded by means of interview, questionnaire, form or telephone call.
Recorded Information	Information that is recorded or stored by graphic, electronic, manual, automated or other means

1.0. Managing of Personal Information Data

1.1 Notice of Privacy

GWC provides notice about privacy policy at the time of customer engagement (e.g. customer information sheet, customer feedback, quote confirmation and approval, contract signing). A mail disclaimer shall be posted on all outgoing GWC email communication and available on GWC homepage.

1.2 Collection

GWC collects the basic contact information of clients and customers including their full name, address, email address, contact numbers etc. for the information relates directly to and mandatory to the organization's operational activity relevant to the purpose for which it is being collected.

GWC does not authorize or permit an outside agent to carry out the collection on its behalf. GWC employee or authorize representative attending the customers shall collect such information through accomplished forms/hard copy information as well as electronic data. Other source of Personal Information may include the following:

- Information provided to GWC through telephone or in person
- Information provided when visiting GWC website or through email
- Information collected through survey either through electronic or hardcopy
- Information from authorized person to provide such information to GWC

1.3 Use and Retention and Disposal

Personal data collected from customer or client shall be used by the company for the purpose of the following information:

- To provide services through response inquiry
- Conduct customer satisfaction survey
- Compliance with legal requirements
- To provide updates and notices on GWC products and services

GWC ensures that all personal data under its custody are protected against any accidental or unlawful destruction and shall be limited to authorized users as outlined in the policy.

All information gathered shall not be retained for a period longer than five (5) years.

All soft and hard copies of personal information shall be destroyed and disposed of in accordance to the GWC policy on waste disposal.

1.4 Choice and Consent

GWC shall not collect, use or disclose personal information without the consent. In other cases, GWC provides opt in/opt out choices or obtain consent to customer/client how to use the collected data. Customer shall have the right to report for any misuse on his/her personal information, update or delete your personal data on GWC records.

1.5 Access to Personal Information, Permission and Sharing

Access to personal data shall be restricted to officers and employees who have specific authorization and a clear business need for that information.

All confidential data shall be clearly labeled as 'Confidential' by writing on the Word/Excel/Power Point document.

In case customer would like to update, delete his/her information, customer shall request in writing or email to Customer Service Supervisor/Manager.

Access through system (laptop, phone, desktop, tablet etc.) shall comply with the security requirement as outlined in the Information Security Manual Standards (*ISO 27001:2013*) for data access.

1.6 Disclosure and Public Posting

Data shall not be disclosed without approval/consent from an authorized personnel. Personal data under the custody of the GWC shall be disclosed only to authorized recipient or in accordance with legal purpose.

All GWC employees and personnel shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession even after resignation or termination of contract through Non- Disclosure Agreement signed by the employees.

Mobile phones with camera and video capability shall not be allowed to be used in GWC restricted areas and customer's premises prior to or during work related activity.

1.7 Disclosure to Third Party Service Providers

A contractual agreement (or MOU if governmental agency, Non- Disclosure Agreement for vendors, suppliers, outsourcing and subcontracting company) outlining security responsibilities shall be in place and approved by GWC Human Resource and Finance Department before exchanging data with the third party / service provider.

1.8 Monitoring, Implementation and Evaluation

GWC QHSE Management System provides framework for all the services and operations as well as providing guidelines and standards in coordination with Quality Assurance and Control Department that ensures supervision with the support of Human Resource and IT.

2.0 Physical Security Measures

This clause includes the procedures intended to monitor and limit access to the facility containing personal data which includes the activities. This is to ensure that tampering and alteration of personal data under the custody of GWC is protected from external access, power disturbances, emergency situations and other similar threats.

2.1 Data Classifications to be collected

The classification of data that are received, stored and transmitted within the custody of the organization are categorized in digital/electronic format and paper based/document information.

GWC Company requires the protection of certain types of data and other information taking into account of any relevant legal or regulatory requirements or contractual obligation.

2.2 Storage type location

All personal data being administered/handled by the organization shall be stored in a data room, where paper based documents are kept in locked filing cabinets.

Digital/electronic data files shall be stored in desktop computers/laptop with password protected provided by the company.

All digital/electronic data shall be stored and backed up in share point or shared folder approved by Department Manager and IT Manager.

2.3 Granting access to unauthorized personnel

Only authorized personnel or employees shall be allowed to access the facility or storage room. Each authorized personnel or employees shall be given a duplicate of the key storage facility room.

Other personnel who wishes to access the facility or storage room shall be given access through authorization request form authorized and approved by Department Supervisor/Manager.

2.4 Monitoring of access facility or storage room

A logbook register shall be in placed at the entrance or facility which indicates the time, date, duration and purpose of each access.

2.5 Personnel involved, Office space/work station design

Desktop computers and/or laptops are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data. Any GWC authorized personnel involved shall always maintain confidentiality and integrity of personal data.

Any GWC staff or employee involved are not allowed to bring their own gadgets or storage device of any form when entering GWC restricted storage room or when entering customer premises.

3.0 Technical Security Measures

The organization shall implement technical security measures in place to ensure that there applicable and adequate protections to secure the processing of personal data, particularly the computer network in place, including encryption and authentication process that control and limit access as specified in GWC Information Security Management System (ISMS) Policy Manual.

(Reference is made to IT ISMS Policies Manual)

A. RECORDS AND REFERENCES

Forms	Description
GWC-IMRS-FM-CIS	Customer Information Sheet
GWC-IMRS-FM-CFF	Customer Feedback Form
System Generated	Quotation Proposal

B. REFERENCE MATERIAL AND EXTERNAL REFERENCES

ISO 9001:2008	Quality Management System
ISO 14001: 2007	Environmental Management System
OSHAS 18001:2007	Occupational Health & Safety Management System
ISO 22000:2005	Food Safety Management System
ISO 27001:2013	Information Security Management System
Eternal Document	Qatar Law Number 13 of 2016
GWC-IMRS-SOP-003	Procedure for Removal Export Movement
GWC-IMRS-SOP-004	Procedure for Removal Inbound Movement
GWC/ISMS/SOP/IT/003	Procedure for IT Backup

C. REVISION HISTORY

Revision	Description	Released By	Details/Description
00	September 30, 2017	QD	Initial Release