GIG GULF

Policy handbook

Personal Cyber Insurance

CYBER INSURANCE

Table of contents

1 Welcome to GIG Gulf Insurance

Thank you for choosing GIG.

This is your Personal Cyber Insurance Policy. This Policy is specially designed to protect you and your family from the financial losses and liabilities associated with cyber-related incidents for individuals.

In this booklet, you will find the wording of your Cyber Insurance. It tells you what is covered and what is not, as well as the conditions which apply and the basis on which all claims will be settled. This Policy and the Schedule are the evidence of the contract of insurance. Please read them carefully, keep them in a safe place.

On receipt of your Policy

To ensure that your Policy gives you the you need, we recommend that you read it carefully in conjunction with the attached Schedule, and return the Schedule immediately if any details are incorrect.

Availability of Cover

This Policy is available only if you are a citizen or have resident status within the UAE, Bahrain, Oman or Qatar where the policy is issued.

Plan Chosen

Your Schedule specifies the plan you have chosen. The Plan names are as follows:

- Luxury
- Premium
- Comfort
- Smart

The plan can be offered as part of Home, Travel, or Personal Accident products, or sold separately as a standalone option.

2 Your Policy Cover Summary

Benefits	Luxury	Premium	Comfort	Smart
Monitoring (Platform access)				
Personal Data Monitoring and Device Protection	Optional	Optional	Optional	Optional
Financial Protection	**Aggregate Limit** AED/QAR 55,000 BHD/OMR 5,500 **Excess** AED/QAR 400, BHD/OMR 40	**Aggregate Limit** AED/QAR 36,000 BHD/OMR 3,600 **Excess** AED/QAR 400, BHD/OMR 40	**Aggregate Limit** AED/QAR 18,000 BHD/OMR 1,800 **Excess** AED/QAR 400, BHD/OMR 40	**Aggregate Limit** AED/QAR 7,000 BHD/OMR 700 **Excess** AED/QAR 400, BHD/OMR 40
Direct Economic loss due to Identity Fraud/ Theft	AED/QAR 36,000 BHD/OMR 3,600	AED/QAR 18,000 BHD/OMR 1,800	AED/QAR 11,000 BHD/OMR 1,100	Not Covered
Online banking / credit cards frauds	AED/QAR 36,000 BHD/OMR 3,600	AED/QAR 18,000 BHD/OMR 1,800	AED/QAR 11,000 BHD/OMR 1,100	AED/QAR 7,000 BHD/OMR 700
Loss on Internet Purchase or Online Purchase	AED/QAR 36,000 BHD/OMR 3,600	AED/QAR 18,000 BHD/OMR 1,800	AED/QAR 11,000 BHD/OMR 1,100	Not Covered
Cyber Bullying, Cyber Stalking and Loss of Reputation	AED/QAR 7,000 BHD/OMR 700	AED/QAR 7,000 BHD/OMR 700	Not Covered	Not Covered
Assistance / Support				
24/7 Cyber Assistance	Covered	Covered	Covered	Covered
IT Assistance	Covered	Covered	Not Covered	Not Covered
Legal Referral (Referral only but not any legal cost)	Covered	Covered	Not Covered	Not Covered
Data Recovery & System Restoration Assistance	AED/QAR 7,000 BHD/OMR 700	AED/QAR 7,000 BHD/OMR 700	Not Covered	Not Covered

Table of Benefit in AED/QAR/BHD/OMR, if the plan is sold in local currency limits (embedded or standalone)

3 Important Information

We would like to draw your attention to important features of your Policy including:

Compensation limits

The compensation limit agreed in the special section applies to the individual insured event. In addition, the assumption of costs for all the insured events within an insurance year is limited to the maximum compensation specified in the Certificate of Insurance.

If the compensation limit agreed for the individual insured event or the agreed maximum annual compensation is not sufficient, you can commission the Assistance Company to provide additional services at your own expense. In this case, the Assistance Company will invoice you separately for the amount exceeding the insured benefit.

Contract

The insurance agreement becomes effective upon your application's submission and the reception of the insurance policy. Your insurance coverage commences on the effective date as mentioned on your policy schedule.

Insurance cover

Insurance coverage will run during the Period of Insurance specified in the Certificate of Insurance.

However, there shall be cooling-off period of 7 days after policy purchase, during which the Insurer shall not be liable to settle any claims that may have occurred during the cooling period or prior to the start of the insurance policy. Only claims pertaining to any events as described hereinunder, occurring after the conclusion of the cooling period, shall be eligible for any settlement.

Cancellation

You can terminate your insurance coverage at any time by providing the Insurer written notice. The termination shall take effect on the date specified on the notice or, if no date is specified, on the date the notice is received by the Insurer.

The Insurer may terminate your policy by providing notice to you at least 30 days prior to the effective date of the termination.

In case of termination by the Insurer or by you, the premium will be refunded to you pro-rata basis within 30 days after the effective date of termination, less an administration fee of AED 50/QAR 50/BHD 5/OMR 5

Premium

Premium is the amount payable by You the insured to Us the Insurance Company.

Legal consequences of non-payment or late payment of the first premium

If you do not pay the premiums for your contract on time, we will cancel your policy from inception and the policy will be treated as null and void.

Law and Jurisdiction

- The law of the UAE, Qatar, Bahrain, Oman where the policy is issued applies to the contract.

This Policy applies only to judgments delivered by or obtained from a court of competent jurisdiction in the country where the policy has been issued.

Conditions and Exclusions

Special Conditions apply to individual Chapters of your Policy, whilst General Exclusions and General Conditions will apply to the whole of your Policy. Refer also to ‘What is not covered’ which applies to each Chapter of the Policy. Additionally, specific claims procedures, which apply to certain Chapters of the Policy, must be followed in order for a claim to be accepted.

Material Fact

All material facts must be disclosed to us. Failure to do so may affect your rights under this Policy. A material fact is a fact that is likely to influence the acceptance or assessment of the risk, including ascertaining the premium by us.

Policy Document

The Policy Document is a crucial piece of information for both the policyholder and the insurer, as it serves as a reference point for understanding the terms of the agreement and the scope of coverage. It's important for policyholders to thoroughly review and understand the Policy Document before purchasing an insurance policy to ensure that it aligns with their needs and expectations.

Policy Limits

"Policy limits" refer to the maximum amount of coverage that an insurance policy provides for specific types of claims or events. These limits are predetermined and outlined in the insurance policy document.

Schedule

The validation page attached to this Personal Cyber Insurance Policy setting out the name of the Insured, Period of Insurance, Chapters insured, Sums insured and other particular or special conditions and terms applying to your insurance.

4 Definitions

Any word or expression to which a specific meaning has been attached will bear the same meaning throughout this Policy.

Assistance Company

means: GULF ASSIST CO.W.L.L, provided by the Insurer for the purpose of servicing the benefits described in the policy, directly or by means of its network.

Bank account

an account with a bank or other financial institution licensed to operate in the Country in accordance with the provision of Central Bank Law where the policy is issued.

Children

means: Persons from 0 months to 18 years old.

Claim

means any event whose consequences are totally or partially covered by the guarantees of the respective Policy Material. The collection of damages arising out of one event constitutes one loss/ accident

Co-insured

means: spouse and children of the Policyholder (up to 5 members) mentioned on the Policy Document.

Company/Insurer/We/ Ours/Us

Gulf Insurance Group (Gulf) B.S.C. (c) henceforth termed as GIG in this document for easy reference.

Cooling-off period

During this period, the insurance provider is not obligated to process or cover any claims that might have arisen either within the cooling-off period itself or before the insurance policy officially commenced. Essentially, this period allows the policyholder to make sure they are content with their policy choice and provides a window for potential changes or cancellations before the policy becomes fully effective.

Cyberbullying

means: Online harassment using electronic communication by sending or publicly posting messages that are intimidating or threatening in nature toward the Policyholder that results debilitating emotional impact and damaged reputations.

Cyber incident

any malicious act or malware occurring on your personal devices.

Cyber stalking

means: Is the use of unconventional or illicit digital technology by gaining unauthorized access to Policyholder's digital device, computer system or computer network of the to track and attack the insured including harassment, embarrassment and humiliation of the insured.

Data

any digital information, irrespective of the way it is used, stored or displayed (such as text, figures, images, video, recordings or software).

Email spoofing

means: Sending email messages with a fake sender address which therefore spammer or other malicious actors is able to change the metadata of an email.

Expert

any person or legal entity appointed by or in consultation with us and/ or the incident response provider (such as an IT, lawyer or public relations consultant).

Excess

The amount you will have to pay towards any claim.

Family

means: Spouse and children up to 5 members.

Fraudulent Claims

means When the Insured Person, Beneficiary or someone acting on their behalf, uses any fraudulent means or devices in order to obtain any of the benefits of this policy, consequently, any payment of any amount in respect of such claim shall be cancelled.

Geographical Limits/ Territorial Limits

Within UAE, Kingdom of Bahrain, Qatar or Oman as stated in your Policy Schedule.

Hardware

the physical components of any personal devices used to store, record, transmit, process, read, amend or control data.

Identity theft

the theft of personal data over the internet, which has resulted or could reasonably result in the wrongful use of such personal data.

Improper use

means: a conscious and voluntary disregard of the need to use reasonable care, which is likely to cause a financial loss.

Insured event

any theft of funds, cyber incident affecting your personal devices, identity theft, cyberbullying, cyber stalking, financial loss due to online shopping and third party claim.

Legal costs

any costs, expenses and/or fees for experts, investigations, court appearances, surveys, examination and/or procedures that are necessary for your civil, administrative and/or criminal proceedings. This does not include your general expenses (such as salaries and overheads).

Limits of liability

as stated in the schedule, including any sub-limit and aggregate limit of liability.

Loss of reputation

any adverse effect on your reputation due to a publication on the internet by a third party.

Malicious act

any unauthorised or illegal act of a third party intending to cause harm to or to gain access to, or disclose data from personal devices through the use of any personal device, computer system or computer network including the internet.

Malware

means: Malicious software, refers to any intrusive software developed by cybercriminals (hackers) to steal data and damage or destroy computers and computer systems.

Mobile wallet

means: any online account in which you deposit or earn money which is denominated in a specific currency that can be spent in a (online) store.

Negligence

means a conscious and voluntary disregard of the need to use reasonable care, which is likely to cause foreseeable grave injury or harm to persons or a property

Personal data

any information relating to a data subject who can be identified, directly or indirectly, in relation to

other information (such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person) as defined by applicable data protection laws.

Personal devices

any devices (computers, laptops, tablets, mobile phones, etc.) used for the purpose of creating, accessing, processing, protecting, monitoring, storing, retrieving, displaying or transmitting data. The term personal devices shall not encompass any smart home devices.

Phishing email

means: When the perpetrators obtain confidential access and / or identification data from unsuspecting third parties with the help of falsified e-mails by exploiting the trust they have gained through deceiving their actual identity. The perpetrators then commit unauthorized actions in online payment transactions using the identity of the person authorized to do so.

Policy

the schedule and policy.

Policy period

means: The period of insurance stated in the Schedule during which the Insurer shall provide the Insured Customers with the Insurance Services. Cover Period starts on the Entry Date and continues for the number of calendar months as specifically stated in the Schedule.

Policy holder

means: The natural or legal person who subscribes this policy with the Insurer and who is bound by the obligations arising therefore, save those which, owing to their nature, must be complied with by the Insured Person the Policyholder/insured persons are addressed as: "You".

Premium

means: The price of the insurance that the Policyholder must pay the Insurer in consideration for the Coverage of the risks provided for the Insured Person by the latter, the receipt for which will include, moreover, the surcharges and taxes legally applicable.

Psychological assistance and treatment

the involvement of an accredited psychiatrist, psychologist or counsellor chosen by you at your own discretion with the prior written consent of us, not to be unreasonable withheld or delayed, to treat you for stress, anxiety or such similar medical conditions.

Robbery

means: loss or damage to a property due to coercion, violence, or the threat of violence.

Service provider

the legal entity stated in the schedule.

Smart home devices

any devices or IoT components used by you in your household in order to operate or control smart home enabled devices such as cameras, air conditioning, lighting, alarming systems or fire protection systems.

Sum Insured

The amount shown in the Schedule representing the maximum amount payable for any number of claims arising out of one occurrence.

Software

any digital standard, customised or individual developed program, or application held or run by a personal device that comprises a set of instructions that are capable, when incorporated in a machine readable medium, of causing a machine with information processing capabilities to indicate, perform or achieve a particular function, task or result.

Social Media

means: platforms, websites and applications that focus on communication, community-based input, interaction, content-sharing and collaboration.

Social Media Account

means: a social media account is a personal or business account that is created on a social media platform.

Spouse

means: Person officially registered as wife or husband of the Insured.

Theft

means: when someone steals your identity and takes out loans or credit cards or applies for services under your name.

Theft of funds

any unauthorized electronic transfer of money, assets or any other funds.

Third party

means: the unrelated or disconnected party to the insurance policy who may bring a legal liability claim against the Policyholder.

Third party claim

any written demand or assertion for compensation or damages by a third party against you

5 Covers and Exclusions

CHAPTER A – DIRECT ECONOMIC LOSSES DUE TO IDENTITY FRAUD / THEFT

What is covered

- The insurance covers the financial losses you suffer because of misuse of your identity. This is the case if a third party uses your personal data to gain a pecuniary advantage by pretending to be your identity, and this results in pecuniary damage.
- If there is a case of identity fraud or theft that leads to a direct financial loss, we will provide compensation for:
  - lost wages due to taking unpaid leave for legal proceedings or criminal investigations,
  - expenses related to correcting records with banks or legal entities,
  - costs associated with postage and phone calls beyond the usual rate plan for reporting the identity theft to legal and financial authorities.

To claim compensation, the policyholder must furnish the relevant report to the appropriate local authority where the incident occurred. The insurance provider might also stipulate submission of the report to the local police authority.

But not

- Theft or robbery of cash or any other property.

How much we will pay

Please refer to the Table of Benefits as mentioned on your policy schedule.

CHAPTER B – ONLINE BANKING / CREDIT CARDS FRAUDS

What is covered

The insurance covers the financial losses you suffer because of fraudulent use of your credit card or debit card or online account takeover, including phishing and spoofing abuse practices. Theft or fraud should be notified to us within maximum 24 hours..

The insurance covers abuse from:

- Your private payment cards (e.g., credit, bank, other debit cards such as EC cards or customer cards with a payment function) for cashless payment for goods and services.
- Your card data for payment transactions (also on the Internet).
- For online banking or e-payment (use of other online payment systems with a bank function).

The prerequisite for the insurance benefit is that you have tried first to get your bank/institution holding the payment means reimburse the fraudulent transaction and are able to provide evidence of that first claim and following denial from the bank/institution holding the payment means. Insurance coverage also applies if the damage occurred during private online banking activities or online payment transactions that you carry out on your registered & own laptop / PC or other personal mobile device (e.g., tablet or smartphone). In particular, damage caused by phishing is insured.

But not due to

- The improper use of
  - Debit, credit, or customer cards.
  - PIN or TRN.
  - Real bearer or identity papers.
  - A digital signature.
  - Other identification or legitimation data arise if the data, cards, or documents came into the possession or knowledge of a third party prior to the conclusion of the insurance or were lost prior to the conclusion of the insurance (no reverse coverage); this also applies if you are not (no longer) aware of where it is
- That you enabled or intentionally brought about with fraudulent intent (e.g., by deliberately disclosing personalized security features such as PIN, TRN, digital signature, etc.).
- Which only lead to damage because you have deliberately not carried out or initiated the check and determination of an unauthorized payment in time.
- Through the loss of cash, electronically stored money, or virtual means of payment (e.g., Bitcoins) from your possession or the possession of a co-insured person.
- In connection with billing from telephone or internet providers.
- That arose as an indirect consequence of an improper disposal, e.g., lost profit or loss of interest or costs incurred for legal prosecution.
- That a co-insured person incurs because of an improper disposal by you or another co-insured person.
- Any kind of ATM cash withdrawals
- Any event following a breach of the information systems from the bank/ institution holding the payment means (i.e. if the bank is victim of a security attack leading to customer data breaches and massive phishing campaigns towards their customers, it is the banks responsibility not ours, their own professional insurance shall cover such event).

How much we will pay

Please refer to the Table of Benefits as mentioned on your policy schedule.

CHAPTER C – LOSS ON INTERNET PURCHASES OR ONLINE PURCHASES

What is covered

Insurance provides cover for

Non-delivery or incorrect delivery of goods purchased over the Internet and in the event that the goods arrive at your location damaged or destroyed. This does not apply if the purchase of a damaged or destroyed item has been agreed or if there is no warranty obligation on the part of the seller for other reasons. A non-delivery exists if you as the buyer have not received the goods within 30 days of the invoice date after full payment. A wrong delivery occurs when goods other than those agreed in the sales contract have been delivered.

The insurance covers goods which are for personal and therefore not commercial or professional use, and which have been paid for in full in one payment process (no hire purchase or leasing). Event tickets (e.g., for theatre, musical or concert visits) are not considered goods in this sense. Hotel booking and flight tickets are also not considered as goods in this sense and are not covered.

- The prerequisite for the insurance benefit is that you have demonstrably asserted the rights to which you are legally or contractually entitled (revocation and warranty rights), at least out of court.
  - To receive faultless goods in the event of damage to the goods through repair or subsequent delivery by the seller.
  - In the event of non-delivery or incorrect delivery, to obtain a new, fault-free delivery of the item by the seller.
  - In the event that a repair or subsequent delivery is not carried out or fails, to have the purchase price reimbursed by the seller after withdrawing from the contract or by way of compensation. A reasonable deadline for out-of-court assertion must have elapsed without success or facts are known that promise no prospect of success.

How much we will pay

Please refer to the Table of Benefits as mentioned on your policy schedule.

But not

For online sales contracts for:

- Cash (including gold and silver coins), Cheques, all other securities
- Transport Tickets, tickets to cultural events, hotel bookings
- Goods from telephone or internet providers (e.g., subsidized mobile phones or tablets, SIM cards)
- Electricity, gas, plants, and animals
- Weapons
- Illegally acquired or prohibited goods
- Jewelry, precious stones
- Glasses
- Mobile phones
- Objects destined for resale

Furthermore, there is no insurance cover

- In the event of damage in connection with online contracts for services, downloads, (software) licenses or copyrights and trademarks.
- For lost profits or interest losses
- For legal prosecution costs that you incur because of asserting your claims (e.g., purchase contract performance, warranty, or damage claims)
- In the event of any loss, damage, or liability arising directly or indirectly from the seizure, confiscation, detention, delay or destruction of any goods by customs authorities, border control, or any other governmental or regulatory agency.

What special obligations do you have?

If the purchase contract is then properly fulfilled, you must reimburse us immediately for the compensation amount received from us.

CHAPTER D – CYBER BULLYING, CYBER STALKING AND LOSS OF REPUTATION

What is covered?

- Management Reputation
  - You will be able to request the removal of any unwanted personal data (written content, photograph or video) from the Interned as being considered wrong, defamatory or simply being issued without your permission, and in compliance with local legislation in place at any given time.
  - You will have to inform us in written of the webpages (social networks, blogs or websites of any kind) where the personal data has to be deleted.
  - In the event that the website refuses to remove the indicated personal data, you will be informed of the options available and may choose to file a legal claim, report the dispute to the local qualified authority, or carry out other actions.
  - Depending on the characteristics of the webpage, such as the country where the company that manages it is located or the transparency of those responsible for it, our service may not be effective and we do not guarantee that any results will be obtained.

The service is available during business hours.

- Psychological Support
  - In the event of a cybercrime, an attempt to the online reputation, defamation or cyber bullying, having consequences on your emotional state or mental health, the Assistance Company will provide psychological guidance and advice to help you cope with the situation.
  - If need be, you will be referred to a psychologist of the Assistance Company network to engage in an in-depth treatment.
  - The service is provided by telephone during business hours.
- Legal Support
  - In the event of a cyber crime, an attempt to the online reputation, defamation or cyber bullying, the Assistance Company will provide you legal support in the settlement of your dispute.
  - The service includes information on rights and obligations, legal actions and procedures to take in relation to the events covered. If need be, you will be referred to a law professional of the Assistance Company network to engage the necessary actions.
  - The service is limited to local country legislation and provided by telephone during business hours. Drafting of reports or opinion is excluded.

How much we will pay

Please refer to the Table of Benefits as mentioned on your policy schedule.

CHAPTER E – IDENTITY PROTECTION PORTAL (IDP PORTAL)

What services do we provide as part of the Identity Protection Portal (IDP Portal)?

In order to design the reputation management effectively and to enable you to recognize abuse, the insurance includes access to the Identity Protection Portal. With the help of our IDP portal you can preventively protect your personal data on the Internet by monitoring and searching for it (online monitoring) and by clarifying problems and questions via the Expert Assistance Hotline or on a self-help basis through the IDP Portal. The portal serves as an early warning system to protect you from data misuse by third parties on the Internet. In addition to the following provisions, the general terms and conditions of the IDP portal and the services detailed apply.

The service is available up to the number of IDs and devices as mentioned in the selected plan.

i) Registration and search function

You will receive access to the portal via a link by email and can log in after assigning a password. Then you have the option of entering personal data to be monitored for on the Dark Web. You can enter the following data there, for example:

- Name
- Address
- Date of birth
- Phone numbers
- E-mail addresses
- Credit cards and bank account numbers
- National Identification number
- ID data (driver's license, identity card, passport)
- Social media accounts

The stored data is searched for at least once a day in the deep web and dark web - automatically and individually. A dashboard shows the level of online risk.

Alerts and monthly reports

You will immediately receive a notification by e-mail if there is any suspicion of data misuse about the stored data. The messages are also visible in the IDP Portal (Identity Protection Portal), whereby the name and date of accounts breached as well as remedial suggestions are displayed.

If you receive a warning, you can contact our Expert Assistance Hotline (see 1.3) for advice on further steps to prevent further abuse and, if necessary, to restore your identity through reputation management (see section A.) (it does not concern about legal advice).

ii) Expert Assistance Hotline and FAQ

You can call our Expert Assistance hotline during business hours between Monday to Friday, if you have the following problems:

- Problem's logging into the IDP portal
- Warning messages in the IDP portal
- Questions about identity theft prevention and detection
- Questions about reputation management.

There is no limit to the number of calls that can be made. The answers to frequently asked questions (FAQ) are available in the IDP portal as immediate help.

In addition, the IDP portal has self-help services that are available 24 hours a day, 365 days a year.

iii) Device Security software to download for PC and mobile devices.

For safe Internet surfing, you have the option of downloading the following security software to your PC and mobile devices:

The service is available up to the number of 2 devices for individual policy and 5 devices for family policy.

Device Security Software helps to protect the Users digital data on various devices and the digital identities of included beneficiaries. Device Security Software includes the Antivirus Protection, Online Banking Protection, Digi-Parenting, and Ransomware Protection software. This Service requires account activation to access software/mobile application and software installation.

- Antivirus Protection shall protect the Users from completely new threats that are not yet identified as viruses using artificial intelligence to scan and analyse the behaviour of files downloaded by the Users and blocks them if they are acting in an unusual way. Downloaded files with the biggest potential for harm are checked against the security cloud before they even reach the Users computer or device.
- Online Banking Protection protects the Users online life with many layers of security and helps the Users private information stay protected. The feature secures the connection between the User and their online banking and detects and shuts down all connections and programs it does not consider secure.
- Digi-Parenting helps set healthy boundaries for Users kids' device use. The feature helps parents create a healthy online environment for their children, using tools to set time limits on all mobile apps, control access of mobile apps, find their device location and block certain types of content.
- Ransomware Protection monitors the important folders on User's devices and blocks ransomware from encrypting data in order to demand a ransom fee.

CHAPTER F – 24/7 CYBER ASSISTANCE

We will answer your calls related to:

- Any suspicious activity, of a proven cyber incident.
- Any query related to the object of this contract (services of benefits entitled)

You will be informed of the actions to take for the major concerns / incidents you may be confronted with compromised data, ID

theft, suspicious email or SMS, ransom attempt, cyber bullying. You shall also, where appropriate, deal with any call that requires specialist attention.

The service is available 24 hours a day

CHAPTER G – IT ASSISTANCE

What is covered

- The subject of the insurance benefits, which we provide during business hours between Monday to Friday, by telephone in the field of non-commercial information technology (IT), are advice and support for:

  a. Everyday use of hardware and software including electronic entertainment devices.

  b. Installation and deinstallation of software, updates and service packs.

  c. Advice on hardware performance increase.

  d. Information on new hardware and software.

  e. Implementation of software updates.

  f. Configuration of the operating system and applications (apps).

  g. General advice on hardware and software.

  h. Installation and configuration of new hardware (e.g., printer, scanner).

  i. Assistance with software downloads.

If advice and support over the phone is not possible, we will try to help you via remote access (maintenance via remote control). An IT expert connects to your device (e.g., computer, mobile device) via a link. Before accessing the hardware remotely, you must make backup copies of the data and software stored on the device on an external data carrier. We do not accept any liability for data loss. You are also obliged to keep the original software ready and to ensure that you have the required license from the manufacturer.

Subject to the terms and conditions herein provided, we use our best efforts to provide a solution to the problem but without guarantee of success.

- Help with cyber security

We support you in dealing with the general dangers of internet use:

a. Cyberbullying.

b. Cybercrime, such as phishing or identity theft fraud.

c. Support in assessing whether there is a cyber risk and what further steps should be taken (e.g., deletion of profiles, accounts, data, or photos as well as blocking access, changing passwords or access data).

IT assistance can be used 3 times per insurance year.

But not due to

a. Damage caused by damage to or incorrect operation of the hardware or software by you.

b. Damage that could have been prevented by backing up the data. Before using this service, you must back up your data up to date. In this respect, it is an obligation within the meaning of Condition # 5 of General Conditions and the legal consequences of Condition # 6 of General Conditions apply in the event of a violation.

c. The functionality of the newly installed original software or other third-party hardware and software that are used for online data backup. In this respect, we are not liable for the fact that the data provided for the above-mentioned backups is available to you. The respective contract for the purchase of the original and other third-party software is concluded exclusively between you and the manufacturer. We are not the seller, licensor, dealer, or manufacturer of the software.

d. All damage due to circumstances beyond our control, such as improper use of the online data backup by you.

e. Damage or claims that can arise after an online data backup:

f. Damage from the non-secure storage of the access data and thus access to the online data backup.

g. Damage resulting from the failure to check the online data backup, or not carried out correctly.

CHAPTER H – DATA RECOVERY ASSISTANCE

What is covered?

- We provide you with the software and the associated license for data recovery for a computer including instructions for use as a download if you lose or damage your data or files because of an online attack or virus attack including Trojans, worms, or similar malware. This assumes that you are the owner or lessee of the data carrier concerned.

- If the data cannot be restored as a result, we will refer you to a specialized service provider for data recovery or arrange a call-back with you by the service provider.

- If help over the phone is not possible, we will organize the collection of the device / data carrier / hard drive on which the data to be rescued is located and ship it to the service provider. This creates a diagnosis to determine whether and to what extent a data recovery or recovery is possible. If this is possible, we will cover the costs for data recovery or restoration. Successful rescue or recovery of data is not guaranteed.

But not

- For data or files that are stored on external storage media, e.g., floppy disks, flash / memory cards, CD-R / CD-RW / DVD, tapes and on Raid / IDE / SCSI systems.

- For data or files that contain criminally relevant content or are in your unauthorized possession. The same

applies to data or files that you keep on a restore or installation medium.

- In the event of damage or data loss due to cyber-attacks that spread within a few days or faster, nationwide or across countries, through other already infected computers and are not recognized by the common antivirus programs at the time of the damage, especially if the computer viruses no longer exist Infect supported operating systems.

How much we will pay

Please refer to the Table of Benefits as mentioned on your policy schedule.

CHAPTER I – LEGAL REFFERAL

What is Covered

Referral to Legal Professionals: We will refer you to experienced attorneys or legal experts based on your specific needs and the nature of your legal issue.

Legal Information: While we do not provide direct legal advice, our team can help you understand the legal process and direct you to resources that may assist in your situation.

But not

Legal Advice

This service is limited to providing referrals. We do not offer legal opinions, representation, or advice.

Choice of Counsel

You are under no obligation to retain the services of the professionals to whom you are referred. The decision to hire an attorney is entirely at your discretion.

Cost of Services

Any fees or costs associated with the legal services you choose to pursue will be your responsibility. We are not liable for any charges incurred.

6 General Exclusions

Apply to all our services.

The following are not insured, regardless of the contributing causes:

a) Which are related to a professional or commercial activity.

b) Due to the use or wear and tear of hardware, obsolescence of software and anti-virus programs as well as faulty programming.

c) That occur because no commercially available firewall was installed and / or updated on the device in question.

d) Due to failures, interruptions, or disruptions to external infrastructures (e.g., power grid, internet, telecommunication networks).

e) Through illegally used software and data.

f) By war, war-like events, civil war, revolution, rebellion, insurrection, riot, civil unrest, hostile acts, general strike, illegal strike, confiscation or disposition by high authorities, damage because of pandemics.

g) By nuclear energy, nuclear radiation, or radioactive substances.

h) Due to earthquakes, storms, storm surges or other natural disasters.

i) Through acts of terrorism; These are any kind of actions by people or groups of people to achieve political, religious, ethnic, or ideological goals that are capable of spreading fear and terror in the population or parts of the population and thereby exerting influence on a government or state institutions.

7 General Conditions

You must comply with the following conditions to have the full protection of your Policy. If you do not comply, we may, at our option, cancel the Policy or refuse to deal with your claim or reduce the amount of any claim payment.

IDP PORTAL (IDENTITY PROTECTION PORTAL)

These conditions apply to the performance and use of the IDP portal. The IDP portal contains the following components: online monitoring tool, security package (software for download on PC / Mac/ Android/ioS), and the Expert Assistance Hotline, which is part of reputation management.

1. Authorization to use

You are entitled to use the IDP portal if you have a corresponding insurance with GIG Gulf, with this service component and you are the insured person. Furthermore, only private individuals residing in the UAE, Bahrain, Oman or Qatar who are at least 18 years old are allowed to use it. Use is only permitted for private and not for commercial or other purposes.

2. Registration

Your registration is required to use the IDP portal. You will receive access to the portal via a link by email and can log in after assigning a password.

3. Termination of your IDP account

In the event of a termination or other termination of the underlying insurance contract from which your user authorization results, the benefits of IDP also end. If the usage authorization ends, we will delete your IDP account. You can terminate your registration in the IDP portal at any time while you are authorized to use it. If you inform us of this request by telephone, we will delete your IDP account with us.

You have the option of resuming use at any time for the duration of your usage authorization. In this case, however, it is necessary to re-enter all data and re-register. To receive the new registration details, please contact the Assistance Company. The termination of the registration always includes all services covered by IDP. Separate termination of individual partial services is not possible.

Furthermore, we can refuse you the services of IDP and block your account if you culpably violate an essential condition of these General Terms and Conditions or if there is a legal obligation to do so.

4. Use of the services

For telephone inquiries in the service Centre, you must legitimize yourself as authorized to use the IDP portal, e.g., by giving your member ID or, if applicable, your insurance policy number. In the interests of your own safety, Europ Assistance will not accept any inquiries without correct authorization.

Telephone calls to the IDP service Centre can be recorded. These records are used to be able to process customer inquiries accordingly and to continuously check the service quality of the service Centre. You will be informed of this before the start of the recording. A recording will not be made if you do not agree to this.

5. Scope of services and functions of the IDP portal

DARK WEB MONITORING:

Dark Web monitoring offers you the option of searching for personal data on the Dark Web. This service is used to track down publicly available information, for which you may not be aware that this data is public on the network. The aim of dark web monitoring is to offer you an early warning system to protect your data from being misused by third parties on the dark web.

Dark Web monitoring searches continuously (at least once a day) for unauthorized use of personal data on the Dark Web. Dark web monitoring does not guarantee that all data on the Internet that is searched for with the help of this service will be found.

You can also view your risk assessment and hits at any time in the individual customer dashboard. The IDP portal then continuously searches the Internet to determine whether the data has been published on the dark web. If this is the case, you will be notified by email and SMS.

WARNING MESSAGES ("ALERT")

If your data, such as credit card numbers, bank details etc. are found, you will immediately receive a warning message. This is also visible in the IDP portal ("Alerts Section"). This message informs you that there is an instance of your data found on the Dark Web.

SECURITY PACKAGE

Device Security Software helps to protect the Users digital data on various devices and the digital identities of included beneficiaries. Device Security Software includes the Antivirus Protection, Online Banking Protection, Digi-Parenting, and Ransomware Protection software. This Service requires account activation to access software/mobile application and software installation.

a) Antivirus Protection shall protect the Users from completely new threats that are not yet identified as viruses using artificial intelligence to scan and analyse the behaviour of files downloaded by the Users and blocks them if they are acting in an unusual way.

   Downloaded files with the biggest potential for harm are checked against the security cloud before they even reach the Users computer or device.

b) Online Banking Protection protects the Users online life with many layers of security and helps the Users private information stay protected. The feature secures the connection between the User and their online banking and detects and shuts down all connections and programs it does not consider secure.

c) Digi-Parenting helps set healthy boundaries for Users kids' device use. The feature helps parents create a healthy online environment for their children, using tools to set time limits

d) on all mobile apps, control access of mobile apps, find their device location and block certain types of content.

e) Ransomware Protection monitors the important folders on User's devices and blocks ransomware from encrypting data in order to demand a ransom fee.

GUARANTEE

A guarantee for the

completeness of the search or the finding of unauthorized displayed or used data on the Dark web is not given.

EXPERT ASSISTANCE HOTLINE AND FAQ

You can call our Expert Assistance Hotline during business hours from Sunday to Thursday, if you have the following problems:

a) Problems logging into the IDP portal

b) Warning messages in the IDP portal

c) Questions about identity theft prevention and detection

d) Questions about reputation management.

There is no limit to the number of calls possible. The answers to frequently asked questions (FAQ) are available in the IDP portal as immediate help.

Reputation management: deletion or blocking of data This service helps in the event of justified suspicion to delete information available online that was found through the IDP portal / online monitoring and that was not uploaded to the Internet by yourself and that falsify or discredit your identity or to have it blocked by the provider.

On your behalf, a message (by e-mail / fax or letter) is created and sent to the responsible body (e.g., website operator and selected search engine operator) with the request to delete / block the information you provided as part of a standard procedure.

There is no guarantee that data will be deleted or blocked. Our service provider merely establishes contact with the data publisher and sends them your request to delete / block your data.

The right to erasure / blocking is not checked, and legal advice is not offered. We send a message to the responsible office with the request to remove the corresponding content from the page. This will be done in English language. If an operator has set up its own reporting system for such cases and we should send the application for you this way, the operator may request additional requirements, information, or documents to process the request, which we in this case from You need.

A copy of this message will be made available to you upon request, optionally by email or letter. If the website operator cannot be determined, we will inform you about this.

We check twice, with an interval of three weeks each, whether the disputed data has been removed from the website. If the content complained of has been successfully removed, we will inform you of this and send you the relevant correspondence (primarily by e-mail with a PDF attachment, if necessary, by letter). If the content complained about is not deleted, we will send a message to the responsible office again. If the website operator does not react to the second message or if he refuses to delete it, you will receive corresponding information from us with the correspondence with the website operator.

The search results in the context of online monitoring do not automatically mean that we contact the internet operator without being asked. You can and must initiate the assignment via our Expert Assistance Hotline.

6. Service / communication

During your registration in the IDP portal, you will receive information about our service by email; for extension and / or expiration notifications and maintenance processes.

7. Data protection

The protection of your personal data is very important to us. Please note our data protection information.

8. Your duties of care

You are obliged to correctly enter your profile data such as name, payment details and address and to keep it up to date. You can make changes in your profile yourself. In addition, you are obliged to keep the access ID disclosed by us strictly confidential and not to pass it on to unauthorized persons or to make these unauthorized persons accessible. The input of data from third parties is not permitted. You may only enter your own personal data in the identity monitor.

In addition, the following is not permitted:

a) To copy, adapt, modify, or change the software or parts of the services made available within the framework of IDP.

b) Elements of IDP for infringement of intellectual property (including, but not limited to, copyright or trademark infringement and infringement of name rights through domain names), terrorism, religious fanaticism, racism, abuse, threat, defamatory purposes, bullying, child pornography or any other legal or otherwise to use morally unacceptable purposes.

c) To impair our services, hosts or networks as well as the possibility of use for other customers or to try to do so. This includes, without limitation, flooding networks with email, deliberately attempting to overload a service, or attempting to crash a host.

d) Sending e-mails with misleading or incorrect headers or with information that obscures the origin of the e-mail or that damages or may damage our reputation, the reputation of our contractors or the reputation of other Internet users.

e) Violations of our network security or attacks on the networks, authentication measures, servers, or devices of other systems. This includes attempting to bypass user authentication or security on any host, network, or user account.

f) Sending messages or viruses that damage or possibly damage our systems, the communication systems of our subcontractors or other customers or any other third party.

g) The interception or monitoring of data that is not intended for you.

h) Deliberately entering data that contain viruses, worms, Trojans, spyware, or other malicious programs that are intended to impair the correct functioning of any software or hardware.

9. Liability

We, our representatives, and vicarious agents as well as the cooperation partners responsible for the provision of services

are liable for services from or in connection with IDP according to the following provisions:

In the case of simple negligence, liability is limited to the breach of essential contractual obligations and to typical foreseeable damage. Essential contractual obligations are those obligations, the fulfilment of which enables the proper execution of the contract in the first place and on whose compliance the contractual partner regularly relies on and may rely.

We always try to keep all details and information up to date.

All content is checked at regular intervals and updated if necessary. Despite careful checks, errors may occur in the information. We therefore assume no liability and give no guarantee that the content and information presented are current, true, and complete.

We do not guarantee the services of the cooperation partners used by the customer. Insurance company's liability for incorrectness, incompleteness, and other defects in the services of the cooperation partners is excluded. Any liability due to technical or other malfunctions that may occur is excluded. Liability for no-fault official measures, labour disputes, force majeure, natural disasters, and accidental damage is excluded. All exclusions of liability do not apply if Insurance company is accused of intent or gross negligence, in the case of injury to life, limb or health or in the case of liability under the Product Liability Act.

This liability regulation does not cover claims under data protection law.

10. Choice of law and place of jurisdiction

The applicable law and the place of jurisdiction are based on the provisions of the underlying insurance contract for the use of the IDP portal.

11. Other

IDP's services are offered to you subject to availability. We strive to provide our services without disruptions. Necessary maintenance work, further development and / or other disruptions can limit the possibilities of use and / or interrupt them temporarily. Data may be lost under certain circumstances. The regular and proper backup of their own data is the responsibility of the IDP user.

OBLIGATIONS OF THE INSURED WHEN A CLAIM ARISES

If an insured event occurs, you are obliged to:

a) To contact the Assistance Company immediately by telephone or e-mail after you have become aware of it and to notify us of the insured event in writing.

b) To provide the Assistance Company with all information - in writing on request - truthfully and completely that is necessary to determine the insured event or the scope of our obligation to provide benefits, as well as to enable us to carry out any investigation into the amount of the damage and the scope of our obligation to provide benefits.

c) To submit to the Assistance Company all original documents that we request.

d) To ensure that the damage is averted or reduced as far as possible and to avoid anything that could lead to an increase in the damage and unnecessary costs. In this context, you must obtain and follow the Assistance Company instructions to avert / reduce damage, if necessary, also verbally, by telephone or by email, if the circumstances permit and are reasonable.

e) To assign to the Assistance Company any claims for compensation against third parties up to the amount of the payment made by us.

f) Report damage caused by criminal acts (e.g., trick theft, identity abuse, damage caused by internet or online purchases and sales) to the police immediately.

g) To provide the Assistance Company immediately the police report with a list of any lost items, data, and assets.

h) The prerequisite for the Assistance Company's use is that you contact the Assistance Company's 24-hour emergency number in advance.

BREACH OF AN OBLIGATION

a) If you breach one of the above obligations, we are exempt from payment in an insured event if you have intentionally breached the obligation. In the event of a grossly negligent breach of the obligation, we are entitled to reduce our performance in a proportion corresponding to the severity of your fault. Here you have the burden of proof that you did not violate the obligation through gross negligence.

b) Notwithstanding the above regulation, we are obliged to perform, provided that the breach of the obligation is neither the cause of the occurrence or the determination of the insured event nor of the determination or the scope of our obligation to perform. This does not apply if you have fraudulently breached the obligation.

c) In the event of a breach of an obligation to provide information or clarification after the occurrence of the insured event, our complete or partial exemption from services is subject to the condition that we have informed you of this legal consequence in a separate notification in writing.

FRAUD

We are released from the obligation to perform if you fraudulently deceive or attempt to deceive us about facts that are important for the reason or the amount of the compensation.

BEHAVIOUR OF THE INSURED PERSON

Insofar as your knowledge and behavior are of legal importance according to the above provisions, the knowledge and behavior of the insured persons must also be taken into account.

NEGLIGENCE CAUSING THE INSURED EVENT

a) If you cause the insured event deliberately, we are exempt from payment. If the deliberate causing of the insured event has been determined by a legally binding criminal

judgment against you, the deliberate causing of the insured event is proven.

b) If you cause the insured event through gross negligence, we are entitled to reduce our benefits in proportion to the severity of your fault.

RECOURSE CLAIMS AGAINST THIRD PARTIES

If you have recourse claims against third parties due to an insured event, these are transferred to the Insurer to the extent permitted by law, provided the Insurer has paid you insurance compensation.

CLAIMS EXPIRY

Your claims against us expire within three years. The period begins on the last day of the calendar year in which the claim arose. When calculating the statute of limitations, the period between the registration of the claim with us and our decision is not considered.

DUAL INSURANCE

If the claimed damage is also insured under another insurance contract, the other insurance contract takes precedence. Our obligation to pay only exists if and to the extent that the damage is not covered under the other insurance contract.

CHANGES TO THE CONTRACT

There are no verbal side agreements to this contract. Changes and additions must be made in text form to be effective.

DUTY OF DISCLOSURE

It is a condition of this Insurance that you have disclosed all material facts to us. Your failure to do so may affect your rights under this Insurance. If you are in any doubt about what was material, then you should declare it to us.

COMPLIANCE

You must comply with all the terms, provisions, conditions, and endorsements of this Insurance. Failure to do so may result in a claim being declined or reduce the amount of any claim payment.

SUBROGATION

We are entitled to take over and conduct in your name the defense and settlement of any legal action. We may also take proceedings at our own expense and for our own benefit, but in your name, to recover any payment we have made under this Policy to anyone else.

You agree to subrogate all rights or remedies to GIG for obtaining relief or indemnity from other parties, upon its paying a claim under this Policy, and shall at the request and at the expense of GIG do and concur in doing and permit to be done all such acts and things as may be necessary or reasonably required by GIG for the purpose of enforcing such rights or remedies, whether such acts and things shall be or become necessary or required before or after the indemnification by GIG.

ARBITRATION

If any difference arises out of this Policy GIG shall immediately notify You in writing of your right to refer the difference to arbitration. Such difference shall be referred to the decision of an Arbitrator to be appointed in writing by You and GIG who may be in difference or if we cannot agree upon a single Arbitrator, to the decision of two Arbitrators one to be appointed in writing by each of You and us within one calendar month after having been required in writing so to do by either of us. The Arbitrators shall agree appointment of an Umpire in writing before entering upon the reference. The Umpire shall sit with the Arbitrators and preside at their meetings and the making of an Award shall be a condition precedent to any right of action against GIG. If GIG shall disclaim liability for any claim hereunder and such claim shall not within twenty-four calendar months from the date of such disclaimer have been referred to arbitration under the provisions herein contained, then the claim shall for all purposes be deemed to have been abandoned and shall not thereafter be recoverable hereunder.

POLICY CANCELLATION

If the Policy has already been incepted, no refund will be made. This policy is non-transferable. In case of the sale of the insured object by the first owner, the policy will be automatically voided and cancelled.

SANCTIONS

If, by virtue of any law or regulation which is applicable to the Insurer, its parent company or its ultimate controlling entity, at the inception of this Policy or at any time thereafter, providing coverage to Insured is or would be unlawful because it breaches an applicable embargo or sanction, the Insurer shall provide no coverage and have no liability whatsoever nor provide any defense to Insured or make any payment of defense costs or provide any form of security on Your behalf, to the extent that it would be in breach of such embargo or sanction.

8 Claims Notification

In the event of a claim – Obligation of the insured during or after the occurrence of any covered event:

a) In order to submit a claim request, please reach out to our call center using the below contact details:

   a.1 80009730536

   a.2 support@Cyberior.com

   a.3 Contact us through Cyberior portal. https://cyberior.com/ae/contact-us/

You will be provided with a claims Form, which will contain further instructions on what You will need to provide to process your claim.

In the request of claim You must indicate Your:

- First and last name
- Date of birth
- Address
- Email
- Phone number
- CLIENT. client ID
- Day of ID theft event
- Passport or ID number

The following requirements apply to specific benefits:

1) Direct economic losses due to ID theft

   In case of an ID theft that results in a direct financial loss, You must submit a claim request within 14 days from the date on which the ID theft became known.

   We might ask You to provide additional documents necessary to assess the claim. This can include a police report for the event, documents required for loss of salary in the event of taking unpaid leave for legal proceedings or criminal investigations, cost of rectifying records with banks or legal authorities, postal charges and telephone calls outside of the rate plan to report the ID theft event to legal authorities, financial institutions. You will have to submit these documents before any reimbursement can be made.

   We will also ask You to provide proof that Your bank or any other contractual partners will not reimburse You and that You have no other insurance policy covering this damage.

   It is your obligation, under this Policy, to take reasonable steps to protect your secured devices and data, including protecting access through passwords, installing and regularly updating anti-malware software, as well as installing other security software updates that provided by the device manufacturers.

   If You will not respect the obligations described above, You may lose all or part of Your contractual rights.

2) Online Banking and Credit Card Fraud

   In case of fraudulent transaction(s), You must:

   - contact the bank / institution holding Your account within 24 hours after You become aware of the fraudulent transaction(s) and ask them to block the affected account and / or private credit / debit card,
   - request reimbursement from the bank / institution holding Your account for the loss suffered as a consequence of the fraudulent transaction(s) and/ or any fees charged by them that relate to the fraudulent transaction(s)

   otherwise We may not pay Your claim.

   In case the bank / institution holding Your account refuses to reimburse part or all of the loss suffered as a consequence of the fraudulent transaction(s) or the fees charged relating to the fraudulent transactions, You must submit a claim request within 7 days from the date You received a refusal from the bank / institution holding Your account to reimburse the losses incurred.

   We will ask You to provide the following documents, which We need to assess Your claim:

   - the copy of the bank / financial institution account statement showing the fraudulent transaction(s)
   - proof that the bank / institution holding Your account, or any other contractual partner or insurance contract, has refused to reimburse Your loss and the reason for the refusal

   Additionally, We may ask for additional evidence of Your loss, including but not limited to:

   - any evidence of the suspicious communication (e.g. the email, SMS, etc.) that led to the fraudulent transaction(s);
   - any evidence that the incident has been reported to the relevant legal authority (e.g. The Police).

   Other additional documents may be required to assess the claim. You must provide your full co-operation if We request any other clarifications required by Us to fulfil our claims management procedures.

   If You will not respect the obligations described above, You may lose all or part of Your contractual rights.

3) Data Recovery

   In the event of cyber-attacks, You can request support for recovery of the personal data that has been lost, corrupted, damaged or made inaccessible by You from your personal device.

   We might ask You to provide additional documents necessary to assess the claim.

   You will have to submit these documents.

   If You will not respect the obligations described above, You may lose all or part of Your contractual rights.

4) Legal Support

   In the event of a cyber crime, You can request legal support for the settlement of Your dispute.

   We might ask You to provide additional documents necessary to assess the claim, such as:

   - any evidence that the incident has been reported to the relevant legal authority (e.g. The Police)

You will have to submit these documents.

If You will not respect the obligations described above, You may lose all or part of Your contractual rights.

5) Psychological support

In the event of a cyber crime, having consequences on Your emotional state or mental health, You can request psychological guidance and advice to help You cope with the situation.

We might ask You to provide additional documents necessary to assess the claim.

You will have to submit these documents.

If You will not respect the obligations described above, You may lose all or part of Your contractual rights.

9 Complaints Procedure

At GIG Gulf, we are committed to providing you with the highest level of customer service. We also realise that from time to time, things can go wrong. Therefore, when you are not completely satisfied, we recommend that you contact our dedicated complaints department.

Usually, one of our agents will be able to resolve your issues or queries immediately, however, if you feel the matter requires an escalation, you can file a formal complaint and your complaint will always be treated fairly and confidentially.

You can file your complaint in any of the following ways:

1) Visit our website and register your complaint

   UAE

   Bahrain

   Qatar

   Oman

   When you submit a complaint, we will contact you within (1) one working day to acknowledge your complaint and provide you with a complaint reference number which will be used in all future communications. We will also explain the next steps in the process and provide you with details on how to contact us to discuss your complaint.

Alternatively, should you not have an email address or access to the internet, you can choose one of the following means to contact us:

2) Send a letter to the management at:

   Dubai:
   Gulf Insurance Group (Gulf) B.S.C. (c), P.O. Box 5862, Dubai, United Arab Emirates

   Bahrain:
   Gulf Insurance Group (Gulf) B.S.C. (c), P.O. Box 11442, Manama, Bahrain

   Qatar:
   Gulf Insurance Group (Gulf) B.S.C. (c), P.O. Box 15319, Doha, Qatar

   Oman:
   Gulf Insurance Group (Gulf) B.S.C. (c), P. O. Box 1276, P.C. 112 Ruwi, Sultanate of Oman

3) Call us and request our customer service team to register your complaint:

   UAE: 800 292

   Bahrain: 8000 1060

   Qatar: 800 2921

   Oman: 800 70 292

4) Walk into one of our branches and request our customer service team to register your complaint:

   UAE

   Bahrain

   Qatar

   Oman

We will endeavour to complete our investigation and share with you the outcome of your complaint within (7) seven working days for UAE, Oman, Bahrain and within (5) five working days for Qatar. If this is not possible, we will let you know and keep you updated throughout the process.

If you are subsequently dissatisfied with our final response or any delay in our response (beyond 15 working days), you may refer your complaint to the Insurance Regulator. You can do so by sending the details of your complaint, stating the GIG Gulf Complaint Reference Number, to the relevant regulator:

For all UAE complaints, you can contact Sanadak using the following details:

Website:
www.sanadak.gov.ae/en/

Email:
info@sanadak.gov.ae

Toll Free:
800SANADAK (800 72 623 25)

For Qatar complaints: you can contact Qatar Financial Centre Regulatory Authority (QFCRA) using their online complaint form or the details below:

Email:
complaints@cdrs.org.qa

Telephone: +974 44 95 68 88

For Bahrain complaints: you can contact the Consumer Protection Unit at the Central Bank of Bahrain (CBB) using their online complaint form or the details below:

Email:
complaint@cbb.gov.bh

Telephone: +973 1754 7777

For Oman complaints: you can contact The Financial Services Authority using their online complaint form or the details below:
Email: info@fsa.gov.om

Telephone: +968 24823331

GIG
GULF

UAE: 800 292
Bahrain: 8000 1060
Qatar: 800 2921
Oman: 800 70 292
gig-gulf.com

GLFPL14052025