Acceptable Use Policy
Keeping our IT System Secure

Issue No & Date	Issue 1 01.01.2017	Issue 1, Rev.1 01.05.2019	Issue 1, Rev.2 03.05.2020	Issue 1, Rev.3 03.05.2021	Issue 1, Rev.4 03.05.2022	Signature
Approved BY	MJVR	MJVR	MJVR	MJVR	MJVR	
Reviewed By	GO	GO	TP	TP	TP	
Prepared By	TP	TP	LD	LD	LD	

CONTENTS

1.0 INTRODUCTION

This policy establishes:

- What is, and is not deemed to be appropriate use of company information systems
- How to use GCC IT securely and handle information correctly
- The extent to which GCC IT may be consumed for personal use
- The level of monitoring of GCC IT
- The consequences of breaching this policy.

We are all familiar with the information systems that we use during our working day (email, Internet, file storage access etc). In many cases we might struggle to fulfil our business responsibilities without access to these capabilities. It is important that we keep these information systems safe and sound, secured from cyber threats and free from viruses and other undesirable content. As responsible users, we need to take sensible precautious to avoid being the next victims of cyber-attack.

Whilst cyber-attack can be a very complex issue to understand - you do not need to be a cyber-guru to keep our IT systems secure - you simply need to follow some straightforward rules to safeguard organisational data. Your secure use of GCC's information systems is crucial in helping to keep our sensitive information secure; our business functioning; and most importantly - you and your colleagues safe.

For our use and management of information systems, it is crucial that we comply with applicable law, regulations, contracts and ethics. This is a responsibility for us all. This acceptable use policy applies to all staff worldwide, including those using our IT. This should be supported by local management at all sites worldwide and supplemented with guidelines and policies applicable to individual jurisdictions. As a rule, it will also apply to agency workers, contractors and any joint venture employees and anyone else who operates GCC IT.

Your responsibility is:	Your manager's responsibility is:
• To familiarise yourself with this policy and comply with it. • To understand how you can use GCC IT securely in order to protect our business interests.	• To understand this policy. • Ensure that neither you, nor your team members are asked to work in a way that breaches in this policy.

Deliberate or negligent failure to follow this policy may result in disciplinary action being taken against you, up to and including dismissal.

Important note: This policy applies across all GCC divisions. In the event of a conflict between

this policy and local laws, the latter shall prevail. However local laws may not be used as a reason to lower the security requirements stated in this acceptable use policy.

We will update this policy as necessary and advise you when this happens.

2.0 POLICY TERMS

Here are the principal terms that we use in this policy:

Acceptable use

Using GCC IT for the given business purposes, and 'reasonable personal use' as defined in this section, operating within the law at all times.

Information Systems / Information Technology

Information system refers to computing devices, telecommunications and other equipment used to store, access, transmit, process or print data.

This includes, but is not limited to;

- Hardware, including servers, workstations, desktops, laptops, tablets and smart phones.
- Storage, including mass storage devices (NAS, SAN), USB memory sticks or removable hard drives.
- Networks, including local and wide area networks (WAN/LAN), Wi-Fi and telephony networks.
- Software that is internally or externally provisioned, including Candy, eZOfis, COINS, GCC Portal.
- Audio-Visual equipment including video conferencing, large flat screen displays and visual display units.
- Desk based telephony equipment and mobile devices including mobile / smart phones, voice and text messaging.
- Multi-function devices, specialised printers or plotters.
- Data in both softcopy (electronic) and hard (paper) forms.
- GCC Portal published with Secure Socket Layer protocol

Reasonable personal use

Reasonable personal use is non-GCC business use, at a level that does not impede your ability to perform business duties, consume a disproportionate amount of work time or system/network resource, nor incur GCC cost.

Regulation

A rule defined in law or government order, applying to GCC or a user concerning information or systems (typically exceeding the rules of the policy defined here and within other GCC policies).

Sensitive information

Information that if released could harm GCC interests (or in the case of personally identifiable information (PII), the citizens concerned). This will include sensitive information/data and files with government classifications, personal data, GCC bids, third party data, legally privileged and commercially confidential information. Information Classification and Handling scheme(s) define this type of information further.

Unacceptable use

Using GCC IT in a manner that is:

- Illegal.
- Damaging to our business interests.
- Offensive to others.

User

A User is defined as a GCC permanent, seconded or temporary employee, (sub) contractor or any other individual with authorised access to GCC IT, services and applications.

3.0 SECURE USE OF INFORMATION SYSTEM

3.1 GCC IT – Correct use

You are authorised to use GCC IT information systems for business activities and a reasonable amount of personal use. As a general rule, you should only be using IT equipment or systems to fulfil your job role, however we appreciate that our IT may also be useful to you in your personal life and therefore a limited amount of use is permitted.

Where you are directed to access, process, produce, hold, or send GCC business data, please make sure you only use GCC IT systems, approved applications and data stores, particularly where these are located in the Internet (cloud).

All IT equipment that you are issued needs to be maintained securely at all times, including when not in use. Equipment must be returned to GCC IT when no longer required or at the request of GCC, specifically at the point that you leave our employment. Software and virtual assets also need to be returned.

Please do not:

- Store unauthorised copies of company information, e.g. on your home PC.
- Act illegally, against Qatar regulations, or in a manner that would damage GCC interests.
- Carry out the business of other companies using GCC's IT assets.
- Produce, access or transmit material that is, or may be considered to be offensive, pornographic, defamatory or libellous.
- Perform actions that are, or may be considered to be bullying, intimidating, harassing or discriminatory.
- Inflame already heated on-line discussions, especially if you are feeling offended by the actions of others.
- Breach the 'reasonable personal use' clause.
- Give GCC IT to an external party or GCC staff without a business need to use it.
- Use personal IT, or any other non-approved third party IT for sensitive GCC business.

3.2 Reasonable personal use

Reasonable personal use refers to activities that do not:

- Occupy too much time and distract you from your work duties.
- Interfere with company business directly or indirectly e.g. excessive use of video streaming consuming large network bandwidth.
- Incur additional costs to the business.
- Access, or attempt to access, to inappropriate material e.g. offensive, pornographic, defamatory or libellous.
- Bully, intimidate, harass or discriminate or offend others.

The personal use of GCC IT for is a privilege, which if abused may lead to withdrawal and disciplinary action.

3.3 Accessing GCC IT

Access to GCC Process / Applications / Software can be achieved by requesting I.T. Department with and official request duly approved by the Line Manager for business requirements.

Our IT systems contain much sensitive information and thus we need access to it granted only

to the correct personnel.

When logging into our IT systems, be vigilant to ensure people cannot see your password as you type it.

Make sure you only ever use strong passwords even if this is not mandated by the system. Remember to update any temporarily issued passwords straight away. You should never be asked to divulge your passwords to anyone, so refuse if you are asked. Please report to the IT Service Desk any persistent attempt to gain you login credentials.

When logging on to GCC IT, you must not:

- Share your unique user id, or group user id, with non-authorised users.
- Share your user or group passwords with anyone.
- Reveal your hard disk encryption key (e.g. Decrypted password) to anyone.
- Write down your passwords and leave them where they can be found or with the IT equipment.
- Reuse passwords across differing systems, especially those hosted outside GCC.

You must report to IT Service Desk any compromise, even if suspected, of your password(s).

- Important note: you must not allow others to use your GCC information system accounts.
- You must not use GCC information systems to misrepresent yourself as another person.

3.4 Locking, logging-off & shutting down

When leaving GCC IT unattended, always make sure that you lock it so that it cannot be accessed whilst unattended. At close of each working day ensure that you log off fully, unless there is a business requirement to remain logged on. You should also reboot your workstation/laptop at regular intervals, preferably every day.

Clear your desk and work area of paper-based information at the end of each day. Secure the valuables and sensitive information in electronic or paper format inside the Safe or other forms of secure storage facilities at closing of each day.

3.5 Remote access

Remote access to GCC network can be obtained by requesting I.T. department with official request duly attested by the Line Manager for business requirements. If you've been issued with a remote access account with a password, it is important that you keep the password safe.

You must not:

- Store your remote access password key with your PC.
- Reveal your remote access password to others.

3.6 Using Email

Your email account is issued to you primarily for GCC business and reasonable personal use in line with definitions/guidance given in section 3.1 and 3.2. Personal use should be clearly distinguishable from GCC business and no attempt to gain benefit by association is allowed.

You should always assure yourself of the identity of the person(s) communicating with, particularly if sending sensitive data. If you receive any suspicious emails, or hyperlinks within emails, please report this to the IT Service Desk immediately.

When placing information in attachments, be careful not to inadvertently send more data than you intended, since Office documents can contain hidden objects, comments, history, reviews, tabs, pages, rows or columns that may not be visible, but that could be retrieved.

Any corporate communications should be sent from approved email addresses and must have the prior approval of the Corporate Communications or IT Communications team.

When using your work email account, you must not:

- Send GCC business emails externally to personal email addresses, e.g. xxx@yahoo.com. This includes automated forwarding mechanisms.
- Use a personal email address to send or receive GCC correspondence or information, particularly sensitive information.
- Externally communicate the email addresses of GCC employees without their approval.
- Reply to requests for information from unknown/non-trusted senders.
- Open attachments from unknown / non-trusted senders or in emails that you were not expecting.
- Click on links to web sites from unknown/non-trusted senders or in emails that you were not expecting.
- Create mass email ("spam") from GCC IT or forward any that you have received.
- 'Reply To All' when an email has been erroneously sent to a large distribution. Better to simply reply to the sender, if necessary.

Be aware that email messages and attachments may be read beyond the addressee list you specify and the content could be used in legal or other investigations. Be sure not to

compromise GCC's legal position and consult with legal counsel if necessary.

Sensitive information must be encrypted if being sent by email.

The use of large attachments or large distribution lists should be avoided and IT approval sought if no alternative is available.

3.7 Using social media

Only use approved social media for GCC purposes, using GCC IT, complying with the behaviours given in section 3.1.

You must not:

- Access or use personal or unapproved social media sites for GCC business.
- Make any posting that would damage GCC business, reputation or good-standing.

3.8 Web browsing

If you are browsing the internet using GCC IT, be sure that you only access acceptable websites, and only clicking on hyperlinks for which you know the target website is safe and acceptable.

When posting GCC information to externally hosted systems/websites/cloud services, ensure that the location has been approved for use.

When using the internet/world-wide-web, you must not:

- Open any files or attachments from unknown or un-trusted locations.
- Access unapproved services that are externally hosted, e.g. cloud services.
- Access any sites that are, or likely to be, unacceptable, e.g. offensive, pornographic, defamatory, subversive, gambling. Note that the ability to reach a website from GCC IT does not constitute an approval.
- Any malicious site links comes through emails are filtered.

You should always validate the accuracy of any information that you download from the Internet, especially those that could cause damage if inaccurate, e.g. exchange rates.

3.9 Political views or statements

GCC information systems should not be used to post political views or statements by sending or posting these to any internet based service. Such communications must be undertaken by Group or Corporate Communications functions.

Avoid discussing subjects that some individuals may find sensitive or controversial, such as politics or religion.

3.10 Information management

When accessing, producing, processing, saving or transmitting GCC information you must only use approved GCC IT. In particular, Internet cloud based services must be approved by your business unit and IT. Additionally, you must always comply with the GCC Information Classification and Handling Scheme.

You must obtain authorisation to share, publish, or transmit material which is:

- Known to be, or is potentially, sensitive, e.g. personal information.
- Subject to legal proceedings.
- Subject to legal, regulatory or contractual control.
- Classified or otherwise protectively marked.

If you need to share, publish, or transmit material, you must have approval to do so. Be sure that the recipient details are correct, that they're authorised to receive the information, and that it is correctly classified and marked as such.

When handling information, you must not:

- Delete that related to any on-going or anticipated legal proceedings without the approval of legal counsel.
- Breach copyright, privacy or other laws when producing, accessing, processing, saving or sending information whilst undertaking GCC business

When using electronic media such as a USB stick or CD/DVD to transfer information, you should:

- Be aware of, and comply with, the Information Classification and Handling Scheme
- Use only GCC approved physical media.
- Protect the media during transit or in storage.
- Encrypt any sensitive data.
- Securely delete the information from the physical media or destroy the physical media after the transfer is complete.
- When disposing of the physical media, do so securely using approved methods.

If you leave GCC employment you must return and clearly identify the location of all GCC information that you have used to support our business. All information on GCC IT equipment remains the property of GCC.

3.11 Hardcopy information

When using company printers or fax machines, you must only print out or send information that is required. Always collect your printouts promptly or immediately if it contains sensitive data.

When printing or faxing sensitive data, always make sure you follow the applicable GCC Information Classification and Handling Scheme. When faxing, always confirm with the recipient the receiving number and how many pages will be included.

Paper based sensitive information should be destroyed as soon as finished with by shredding or secure paper waste facility.

3.12 Remote working and travelling

You should always turn off your laptop when travelling or leaving it unattended outside of your work environment. In non-office locations or public places the threat to information from theft or overlooking is much higher and more vigilance is needed. All devices should be physically secured when not in use.

3.13 Monitoring

GCC has the right to:

- Monitor internet access and block access to particular web sites, categories of sites, or specific types of communication.
- Monitor user activity to ensure compliance with this AUP or other information security policy.
- Access and disclose any of your electronic and phone communications.
- Audit IT equipment, software and information at any time without prior notice.
- Monitoring, access and disclosure will only be sanctioned in a proportionate manner justifiable by business need at our discretion.
- For any criminal matters, GCC will reveal information from our IT systems as necessary to support law enforcement authorities.

3.14 IT configuration control

It is essential that GCC IT, including business applications and networks, are only operated in the configuration that they have been issued to you.

Thus, you must not:

- Alter the configuration of GCC IT, including hardware, software, security controls or network equipment without approval.

- Install or connect non GCC approved devices, e.g. USB hard disk drives, network or wireless hubs.
- Download or install unauthorised software.
- Attempt to connect our IT to a GCC network and a non-GCC network at the same time, e.g. to bridge our network to a third party network or the internet.
- Use company SIM cards in personal devices or personal SIM cards in company devices.
- Submit any malicious or malformed data intended to break our applications, systems or software, or bypass any security controls.

You are expected to promptly install any software and anti-virus updates automatically downloaded by IT to your workstation or laptop. You should regularly connect your laptop to the corporate network to receive these.

3.15 Reporting a security breach

If you suspect this policy, or any of our other IT policies or standards have been breached, accidently or deliberately, you must report it to IT Service Desk or the Information Security Function itsupport@gulfcontracting.com immediately.

If you are aware of, or receive material, that is, or may be, illegal, criminal, pornographic, offensive, defamatory, bullying or harassing in nature or discriminatory, then you must report this to the IT Service Desk or the Information Security Function itsupport@gulfcontracting.com immediately

You must not alter, delete or forward the unacceptable material without permission from either the IT Service Desk or the Information Security Function.

3.16 Security Incidents

You must report suspected security incidents (e.g. virus, loss of equipment or information, suspicious email attachment) to the IT Service Desk or Information Security Function itsupport@gulfcontracting.com immediately.

You must not discuss a security incident further, except to report the incident. You are expected to support any incident investigation with the IT Service Desk or Information Security Function.

Where appropriate, a theft should be reported to the local police who will provide a crime reference number that IT will record.

3.17 Cryptographic Controls

Cryptographic controls shall be used when available natively through the authorized software employed at GCC.

For example: The use of SSL (secure socket layer) to access web pages on our servers and IPsec tunnels used natively with Cisco and Fortigate devices.

3.18 Mobile Usage Policy

Refer Clause 5.3.6 in ISMS Policy Manual (GCC/ISMS/M/001 Issue 1 Rev 0) for Mobile usage policy.

3.19 Compliance with the policy

Compliance with this policy, and all future versions, is mandatory for all users with access to GCC IT including those employed by GCC Business Units, Joint Ventures and supplier organisations, as well as secondees, contractors, volunteers and visitors.

Users must declare their understanding and acceptance of this policy below, before access to IT systems will be given.

4.0 USER DECLARATION

I have been provided with a copy of the GCC Acceptable Use Policy and fully understand the terms of the policy and agree to abide by them.

I understand that this policy may be amended and that upon notification of this I will be bound by the latest version.

Should I be a third party accessing GCC information and systems, I will obtain, read and abide by the GCC Information Security Policy and framework of supporting policies.

5.0 DOCUMENTATION

The master copy of this policy shall be filed by the IT Manager together with other policies.