	AUTOMOBILE CORPORATION OF GOA LTD.	
TITLE:	IT SECURITY POLICY, GENERAL GUIDELINES	
PREPARED BY:		PAGE: 1 OF 4
APPROVED BY:		

PURPOSE :
To provide guidelines for IT SECURITY.

SCOPE :
This procedure shall be applicable to all employees of ACGL.

RESPONSIBILITY:
All employees of ACGL using IT infrastructure.

PROCEDURE:

1. *FOR CONTROL OF SYSTEM USAGE*
   1) Don't give out your password to any one, including the system administrator. It's your own and should be guarded carefully.
   2) Don't install any extra software on your system from external sources such as the Internet, or your personal CDs and floppies. This could have malicious code that could destroy data on your system, or even spread it to other systems on the network.
   3) If you find a problem with your PC, don't try to fix it yourself. Call the support staff and lodge a complaint.
   4) Shut down your system when you are leaving for the day to save power.
   5) You have been given a user account and password to login to the file server. Change your password periodically. Do not make your password easy to guess, such as your initials, your wife's, kids or friends name.
   6) Do not store your personal data such as family photos, songs or videos in your home directory on the file server.
   7) In case you need to share files with somebody else on the network, then do not send it by e-mail or share your directory. Put it in the common folder on the file server, and ask the recipient to delete it after taking it.
   8) Do not leave critical documents in the common folder of the file server.
   9) Don't attempt to gain unauthorised access to information facilities. It is an offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you don't have access to information resources you feel you need, contact your IT Support person or provider.
   10) If you leave your PC unattended without logging off, you are responsible for any misuse of it while you're away.
   11) ALWAYS check floppy disks/pen drives for viruses, even if you think they are clean (contact IT Support to find out how). Computer viruses are capable of destroying ACGL's information resources. It is better to be safe than sorry.
   12) Don't forward emails warning about viruses (they are invariably hoaxes and IT Support will probably already be aware of genuine viruses - if in doubt, contact them for advice).

	AUTOMOBILE CORPORATION OF GOA LTD.	
TITLE:	IT SECURITY POLICY, GENERAL GUIDELINES	
PREPARED BY:		PAGE: 1 OF 4
APPROVED BY:		

2. *FOR CONTROL OF INTERNET USAGE*
   1) Do not reply to any spam mail, even if it gives instructions to do so. This will actually confirm your presence to the spammer and you could be spammed even more.
   2) Be wary of opening e-mail attachments, unless you are sure that it is from a reliable source and that you were expecting it. If necessary, call up the sender to check.
   3) Use it in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use. Think and check messages before sending (just as you would a letter or paper memo).
   4) Only send Email to those it is meant for; don't broadcast (i.e. send to large groups of people using email aliases) unless absolutely necessary since this runs the risk of being disruptive. Unnecessary (or junk) email reduces computer performance and wastes disc space.
   5) If you wish to broadcast other non work related information or requests (e.g. information or opinions on political matters outside the scope of ACGL, campaigning, social matters, personal requests for information etc.) it is better to use a Webmail account or a personal email account at home; don't use the standard (work) aliases.
   6) Don't broadcast emails with attachments to large groups of people- either note in the email where it is located for recipients to look, or include the text in the body of the email. Failure to do this puts an unnecessary load on the network.
   7) When publishing or transmitting information externally be aware that you are representing ACGL and could be seen as speaking on ACGL's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager.

	AUTOMOBILE CORPORATION OF GOA LTD.	
TITLE:	**IT SECURITY POLICY, GENERAL GUIDELINES**	
PREPARED BY:		PAGE: 1 OF 4
APPROVED BY:		

3. *FOR CONTROL OF NETWORK USAGE*
   1) In case your system is not able to access the network, do not try to tamper with the network settings and cables. Call the support staff instead.
   2) Trying to access areas that you are not authorized is strictly prohibited, and could have serious implications if you are caught doing it.
   3) Keep master copies of important data on ACGL's network and not solely on your PC's local C: drive or floppy discs. Otherwise it will not be backed up and is therefore at risk.
   4) Ask for advice from IT Support if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring your network to a standstill.
   5) Do not store personal (non- ACGL files) on ACGL's network.