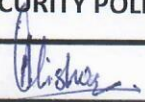
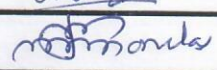
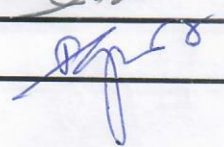


AUTOMOBILE CORPORATION OF GOA LIMITED		 MISP 001
TITLE	IT SECURITY POLICY GENERAL GUIDELINES	
PREPARED BY		Page 2 of 6
REVIEWED BY	 (IT Head)	Rev No. 2
RECOMMENDED BY	 (CTO)	
APPROVED BY	 (CEO & ED)	Date :24-Feb-2025

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 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).
- 13) Select strong passwords to protect your confidential information.
- 14) Use at least 10 characters which include lowercase, uppercase, special characters and numbers.e.g., **Bw!tLao3ek = Blue Whale Is The Largest Animal On Earth Ever Known**
- 15) Refrain from using names, date of birth, or dictionary words as your password.
- 16) Use different passwords for personal and official accounts.
- 17) Follow clean desk policy
- 18) Avoid storing confidential files on removable devices such as USB drives.
- 19) Avoid storing customer information on local systems.
- 20) Lock your computer whenever you walk away from it.
- 21) Don't leave important documents or laptops unattended.
- 22) Don't connect official devices on public Wi-Fi.
- 23) Dispose old IT equipment and records securely.
- 24) Always collect your printed documents immediately from the printer trays.
- 25) Ensure Secure Data Disposal by following points

AUTOMOBILE CORPORATION OF GOA LIMITED		 MISP 001
TITLE	IT SECURITY POLICY GENERAL GUIDELINES	
PREPARED BY	<i>[Signature]</i>	Page 3 of 6
REVIEWED BY	<i>[Signature]</i> (IT Head)	Rev No. 2
RECOMMENDED BY	<i>[Signature]</i> (CTO)	
APPROVED BY	<i>[Signature]</i> (CEO & ED)	Date :24-Feb-2025

- ❖ Destroy old/unused documents in an irretrievable manner.
- ❖ Do not leave unwanted copies at the photo-copier machine. Shred them
- ❖ Submit laptops/smartphones that are no longer useful to the IT team
- ❖ Removable media (CDDVD/USB Drive) containing sensitive data should be physically destroyed before disposal

26) Ensure Mobile Device Security by following points

- ❖ Ensure physical security of your smartphone to prevent theft, unauthorized usage or installation of malware.
- ❖ Enable the smartphone's password/passcode protection setting feature.
- ❖ Install operating system updates whenever they become available.
- ❖ Install an anti-malware protection app (if available for the device) to prevent infection from malicious apps and websites.
- ❖ Do not install applications from untrusted sources
- ❖ Do not save passwords, PINs in your mobile phone.
- ❖ Avoid using public / free Wi-Fi, especially for online banking activities.
- ❖ Turn the Bluetooth / Wi-Fi access feature off when not needed.
- ❖ Avoid opening suspicious e-mail or SMS text messages

27) Ensure IT Asset Security by following below points

- ❖ Always protect your IT devices provided by the company with utmost care.
- ❖ Never leave your official devices unattended.
- ❖ Don't make changes to your official system without concerning approval.
- ❖ Understand that you have ownership of the device in case of damage.
- ❖ Don't delay informing the IT team in case of damage or loss of any IT asset.
- ❖ No pirated software's to be used at organization level.

AUTOMOBILE CORPORATION OF GOA LIMITED		 MISP 001
TITLE	IT SECURITY POLICY GENERAL GUIDELINES	
PREPARED BY	<i>Alisha</i>	Page 4 of 6
REVIEWED BY	<i>[Signature]</i> (IT Head)	Rev No. 2
RECOMMENDED BY	<i>[Signature]</i> (CTO)	
APPROVED BY	<i>[Signature]</i> (CEO & ED)	Date :24-Feb-2025

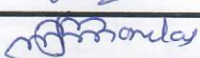
❖ Always backup your official data as per company guidelines

28) Stay Safe from Phishing , Vishing and Smishing by ensuring below points

- ❖ Beware of messages requesting data, a phone call, or an operation.
- ❖ Don't trust attractive offers on emails and SMSes.
- ❖ Don't click on the links or attachments in suspicious emails and SMSes.
- ❖ Never give out personal information on emails, messages, or calls.
- ❖ Enable ad-blocker and pop-up blocker in the browser.

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

AUTOMOBILE CORPORATION OF GOA LIMITED		 MISP 001
TITLE	IT SECURITY POLICY GENERAL GUIDELINES	
PREPARED BY		Page 5 of 6
REVIEWED BY	 (IT Head)	Rev No. 2
RECOMMENDED BY	 (CTO)	
APPROVED BY	 (CEO & ED)	Date :24-Feb-2025

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
- 8) Suspect emails with links requesting information like bank account details etc.
- 9) Avoid saving organization's information on external mail account.
- 10) Internet should be used for business purpose only.
- 11) Do not attempt to visit restricted sites.
- 12) Do not upload confidential/ Sensitive information on social media sites.
- 13) Don't open emails from someone you don't know or trust.
- 14) Don't open unexpected attachments or click on suspicious links.
- 15) Use 'Reply All' option only if necessary
- 16) Never use the 'Remember Me' feature
- 17) Don't give your official email address to strangers.
- 18) Don't use your official email for personal tasks.
- 19) Don't accept friend requests from strangers.
- 20) Don't reveal sensitive personal information on social media.
- 21) Become familiar with the privacy policies of the social media channels you use.

AUTOMOBILE CORPORATION OF GOA LIMITED		 MISP 001
TITLE	IT SECURITY POLICY GENERAL GUIDELINES	
PREPARED BY	<i>[Signature]</i>	Page 6 of 6
REVIEWED BY	<i>[Signature]</i> (IT Head)	Rev No. 2
RECOMMENDED BY	<i>[Signature]</i> (CTO)	
APPROVED BY	<i>[Signature]</i> (CEO & ED)	Date :24-Feb-2025

- 22) Customize your privacy settings to control who sees what.
- 23) Limit details about work history on social media
- 24) Do not engage in illegal or unethical activities including gambling, games, accessing obscene material
- 25) Inappropriate / Offensive material should not be downloaded, viewed, stored, displayed, distributed and edited

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 .Otherwise it will not be backed up and is therefore at risk.
- 4) Ask for advice from IT Support if you need to store, transmitter 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