EASA SALEH AL GURG GROUP

POLICY FOR EMAIL SECURITY

DOCUMENT NO.: ESAG-IT-P-009

REVISION HISTORY

Any revision to this document must be approved by the Group CEO. Any changes to the policy which affects the Delegation of Authorities as set out in this document above the Group CEO must be approved by the Managing Director.

REVISION DATE	BRIEF OF REVISIONS MADE	PREPARED BY	APPROVED BY
Aug 20, 2015	Initial Issue	Group IT	GGM
June 13, 2021	Revised to incorporate new logo and GCEO	Group IT	Group CEO

POLICY EFFECTIVE DATE & DATE OF ISSUE

This document is intended to be issued on June 13, 2021 and is to be effective as of the same date.

1. OVERVIEW

Email security breach is becoming an increasingly significant threat to organizations around the world. Generally the company E-mail systems are a high risk area due to their constant availability to the outside world, and the risk is often two-fold. The use of e-mail to conduct business, contact clients, and its integration in many other business related processes exposes company mail addresses and (mail) systems to potential attackers. Viruses and malwares, of course can sometimes penetrate the firewall by hiding within emails. Once opened, the virus can spread and cause significant damage to internal systems.

2. PURPOSE

The purpose of this policy is to ensure that Easa Saleh Al Gurg Group's e-mail facilities are used in a manner that is fit for business and not illegal, irresponsible or disruptive to ESAG's network facilities, services and infrastructure.

3. APPLICABILITY

The policy will be applicable to all entities in Easa Saleh Al Gurg Group LLC.

4. SCOPE

This policy covers appropriate use of any email sent from ESAG's email address and applies to all employees, vendors, and agents operating on behalf of ESAG. This policy applies to all computing equipment on which ESAG's e-mail services, is accessible either through Email Clients or any Web Browser.

5. DEFINITIONS

Malwares - Short for malicious software, malware is software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.

Firewall - Firewall systems prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

Encryption - The translation of data into a secret code. Encryption is the most effective way to hide data and achieve security.

Spam - Spam is unsolicited or junk e-mail.

Anti-Spam - The phrase anti-spam (or anti-spam) refers to any software, hardware or process that is used to combat the proliferation of spam or to keep spam from entering a system.

Content Filtering - Content filtering is the use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable.

6. POLICY STATEMENT

- E-mail should not be used for intentionally transmitting, retrieving or storing any message with an illegal content; such uses include, but are not limited to:
  Global forwarding of messages to parties inside (all Staff / all department groups) or outside, unless prior permission is obtained from the management.
  "Letter bombing": re-sending the same e-mail message repeatedly to one or more recipients.
  "Spamming": exploiting auto-distribution lists or similar systems for the widespread distribution of uncalled-for email.

Sending propaganda, unethical or hate literature.
Sending or forwarding chain letters.

- E-mail Users should not attempt to read or monitor others e-mail unless authorized.
- E-mail Users should not send Company's confidential or sensitive information outside the Company unless authorized.
- All Company e-mails are owned by ESAG, and ESAG reserves the right to review the contents whenever deemed necessary after obtaining the necessary approval from ESAG's Management. Unless internal transfer or unrecoverable damage happens to Local PC's is involved, no email backup/restore requests will be entertained.
- Users are strictly prohibited from:
    - Sending unsolicited email messages such as chain mail or spam.
    - Forging or attempting to forge email messages, or disguising or attempting to disguise their identity when sending mail.
    - Giving out a password for any type of account via email.
    - using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct ESAG business, to create or memorialize any binding transactions, or to store or retain email on behalf of ESAG
    - Sending emails to any personal email Id's using ESAG's corporate email accounts. If as per business requirement there is no alternative left, ESAG staff should immediately inform the same to IT coordinator with customer and formal approval must be taken before proceeding email communication.
    - Email users are strictly prohibited from sending any emails with attachment of content type .exe, Perl, cold fusion, ASP, PHP etc.

- ESAG information resources shall not be used to transmit or receive statements that contain any material that is offensive, defamatory, or threatening to others.
- Any use of Email from network is traceable to ESAG. Personal sending out any mail outside should keep in mind reputation of ESAG.
- E-mail messages are not encrypted by default and Users should exercise caution by not embedding system or application passwords in their e-mail messages.
- E-mail messages are scanned for viruses on the internal and external e-mail servers. In the event of any detection of viruses, the e-mail message will be deleted from the system and auto generated warning message will inform the recipient or sender for the detected virus along with the taken action.
- Anti-spam and content filtering tools would be used at the e-mail gateway for checking incoming and outgoing mail messages.
- If required and authorized by IT Manager, the guest shall be provided with an ESAG desktop that would have internet and external email facility.
- Personnel should not open emails or attached files without ensuring that the content appears to be genuine. If you are not expecting to receive the message or are not absolutely certain about its source, do not open it.
- Employees must exercise utmost caution when sending any email from inside ESAG to an outside network. Confidential information will not be forwarded via any means, unless that email is critical to business.
- Email User should contact the IT help Desk/Exchange team, through their IT coordinator if any incoming/outgoing mail is been marked SPAM or rejected due to SPAM content.

- No user should create Email signatures of their own under any circumstance. Email signatures are to be generated via central Email system and any design change should be approved by Group Quality & business Excellence and IT department.
- Any email deleted should be made recoverable from deleted items for another 30 days. Mailbox should be maintained for 6 months after an employee id is been disabled. Emails are to be available in journal for 5 years.
- Compliance measurement :

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the Senior Management.

7. BREACH

If any user is found to have breached this policy, they may be subject to ESAG's disciplinary procedure (ESAG-HR-P-003). If you do not understand the implications of this policy or how it may apply to you, kindly seek advice from Corporate IT department.

ESAG IT Security Policy Privacy Statement.

Although ESAG shall strive to maintain the confidentiality of the data in ESAG systems, privacy cannot be guaranteed. Corporate IT department employees shall have access to the business data, e-mails and personal data stored in the ESAG systems as well as in the Mobile devices connected to the ESAG network. Corporate IT department can give access to the relevant data to other corporate departments based on the approvals by ESAG senior management.