1. Purpose

Information plays a vital role in contributing to operational and strategic business decisions, legal and regulatory requirements, core business processes, and customer service. Accordingly, data must be protected to a level commensurate with its value to the AGI.

AGI's Cybersecurity division protects assets from threats and associated risks to its confidentiality, integrity, and availability by assessing, detecting, selecting, implementing, and monitoring security control measures and thereby managing the risks to an acceptable level.

2. Applicability

The control policies listed and stated in this document apply to all staff members, vendors, and customers who handle the Al Ghurair's assets, including but not limited to the information created, processed, stored, or retained by AGI as part of its functions and services regardless of geographical location.

3. Principles

The group provides electronic mail resources to support its business activities. This policy sets out the group's requirements about the use of, access to, and disclosure of electronic mail.

3.1 Policy Statement

E-mail is a corporate resource that must be used solely for purposes that directly benefit Al Ghurair. The use of any group resources for electronic mail must be related to business. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost to the group. Any such incidental and occasional use of electronic mail resources for personal purposes is subject to the provisions of this policy.

- Users should always consider whether E-mail is the most appropriate form of communication. Often telecommunication and face-to-face communication are more effective, particularly where the subject matter is complex or contentious. Users should minimize those copied on the E-mails and address messages only to individuals who need to know the content for the job purpose.
- Only staff who have received permission under the appropriate authority are authorized users of the group's electronic mail systems and resources.
- The Group IT will make efforts to maintain the integrity and effective operation of its electronic mail systems. Users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information.
- The maximum size of the E-mail attachments (30 MB) will be globally restricted to enhance the processing of the email system. For genuine businesses that need to transfer attachments that are of greater size than the system restriction, following alternate secure means such as secure FTP, HTTPS must be utilized.
    - **Microsoft Onedrive (Internal & External).**
    - **Microsoft Sharepoint (Internal & External).**
    - **MS Teams (Internal Only).**
- AGI's electronic mail resources will not be used for personal monetary gain or for commercial purposes that are not directly related to the group's business. Personal use that creates a direct cost for the Group is prohibited.
- Other prohibited uses of electronic mail include, but are not limited to:
    - sending copies of documents in violation of copyright laws
    - forwarding chain letters, spam emails, greeting cards, junk email, jokes, screensavers, non-

business-related PowerPoint slides, images, music files and videos
- using abusive, racial or any other form of inappropriate language or pictures in the content
- sending non-business-related emails to a group defined distribution lists or a huge number of recipients.
- using the corporate email address to subscribe to personal internet mailing lists, automatic feeds, other internet communities and social networking sites.
- sending and receiving business information using personal, unofficial email addresses
- inclusion of the work of others into electronic mail communications in violation of copyright laws
- capture and opening of electronic mail except as required for authorized employees to diagnose and correct delivery problems.
- use of electronic mail to harass or intimidate others or to interfere with the ability of others to conduct Group business.
- use of electronic mail systems for any purpose restricted or prohibited by laws or regulations.
- attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system or attempting to intercept any electronic mail transmissions without proper authorization.

- Users must not share user logon ID's and /or passwords.
- Users must not attempt or intercept any electronic mail that they are not authorized or intended to receive.
- Users must not modify or delete messages or files from within another individual account maliciously or with intent to deceive.
- A user must not alter the content of an electronic mail message originating from another source with intent to deceive.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.10.8.4 Electronic Messaging	A.13.2.3 Electronic Messaging

4. Accountabilities

Role	Responsibility
Manager IT Security	The Infosec team will verify compliance to this policy through various methods, including but not limited to, reporting tools, internal and external audits, and feedback to the policy owner.

5. Definitions

Abbreviation	Definition
AGI	Al Ghurair Investment

6. Waivers and Exceptions

Any exception to the policy must be approved by the Group IT Cybersecurity team in advance.

7. Document controls

Approvals	Name	Designation	Date	Signature
Prepared By	Kamran Manzoor	Manager – IT Security	Oct 2023	Kamran Manzoor Digitally signed by Kamran Manzoor Date: 2023.10.26 15:47:50 +04'00'
Reviewed By	Tabrez Sheikh	Senior Vice President - IT PMO& Governance	Oct 2023	Tabrez Sheikh Digitally signed by Tabrez Sheikh Date: 2023.11.22 11:16:50 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:22:38 +04'00'

Date	Version	Changed by	Description
Oct 2023	1	Kamran Manzoor Manager – IT Security	1st Version.