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

Access to the Internet through the Company is a privilege. Users granted this privilege must adhere to strict guidelines concerning the appropriate use of this information resource. The rules and regulations are in place to protect individuals as well as the organization.

3.1 Policy Statements

While maintaining the safety and security of the corporate networks, arrangements are made for responsible access to the Internet as a major element in the core IT services. The following are criteria that must be observed by people with access to the Internet to maintain an acceptable level of integrity with usage.

- Comprehensive security arrangements are in place to protect the Group. Personnel's must not attempt to disable, defeat, or circumvent these Internet security arrangements. Personnel must not violate this privilege by using access to the Internet for unsuitable purposes that may bring the Group into disrepute.
- Internet access will be through the service provider engaged by the AGI. Accessing the internet from corporate facilities through any other means is prohibited.
- Other prohibited uses of Internet include but are not limited to:
    - usage of peer-to-peer networks such as LimeWire, Kazaa, torrents or any unauthorized internet-based media/file transfer and storage mechanism.
    - usage of sites that facilitate proxy avoidance.
    - usage of sites that facilitate VOIP (voice over IP), streaming audio and video, unless authorized by Group IT Cybersecurity.
    - engaging in any blogging activities that may tarnish the Al Ghurair's Group image, reputation, and good will.
- Personnel who wish to upload, or post or publish material to an Internet site or service must be aware that copyright, trademark, and public speech control laws exist in all countries within which the AGI operates. Care must be taken not to violate any laws that may be enforceable against the Group.
- Employees must not post or place any company material on any publicly accessible computer without prior written permission from Group IT.
- The accessing or displaying of any kind of sexually explicit images or documents on any group system is strictly prohibited. In addition, sexually explicit material must not be archived, stored, distributed, edited, or recorded using the Group's network or computing resources. This restriction extends to racist, and similar material. If any employee finds that they have connected to a site that contains such material, they must disconnect immediately, regardless of whether that site has been previously deemed acceptable by any screening or rating program.
- The Group has software in place that monitors record and recalls all Internet usage and reserves the right to do so.

- Users may download only software and data with direct business use and must arrange to have such software and data properly licensed and registered. Downloaded software must be used only under the terms of its license. No employee with access to the Group's facilities may use them knowingly to download or distribute pirated software or data.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.10.6.2 Security of Network Services	A.13.1.2 Security of network services
A.11.4.1 Policy on use of network services	A.9.1.2 Access to networks and network services

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
VOIP	Voice over Internet Protocol

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 15:49:09 +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 11:18:39 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:23:21 +04'00'

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