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 objective of this policy is to protect information while being transferred through all types of communication facilities.

3.1 Policy Statements

- Removable devices such as USB, memory cards, mobile phone storage, writable CD and DVDs are **blocked** by default on all corporate machines. Wherever there is a business requirement to transport sensitive data, an approval from BU CEO & Group CEO is required.
- All removable media obtained from vendors and third parties will be automatically scanned for malicious code by endpoint protection systems.
- Group IT will implement removable media storage device blocking and monitoring controls via which such devices can be monitored and blocked after consulting with different business entities to demonstrate the business risk versus a defined business need.
- Personal hardware media storage and transportation devices (e.g., mobile phones, PDAs, laptops, other wireless, blue tooth devices etc.) or any non-domain joined device must not be connected to Al- Ghurair's corporate network.
- Group data must not be transported and stored on personal computing devices such as home computers or home laptops.
- Personal laptops, visitor and consultant laptops must only be allowed to connect to dedicated guest networks which are isolated from accessing internal systems.
- All business managers must consider data security risks and assess genuine mobile working needs when approving mobile computing devices such as laptops for employees.

- Users must ensure that all laptop devices and other mobile computing devices are always physically secured.
- Any lost or stolen devices must be immediately reported to AGI IT and Admin departments to enable any appropriate access control revocations as well as to initiate insurance claim procedures.
- Signed agreements such as non-disclosure must precede the disclosure of sensitive information to external parties. Relevant legal departments must be approached for due diligence on such agreements.
- Prior to granting access to any information, Group IT will ensure all users are briefed on information security roles and responsibilities by signing the responsible computing agreement.
- Group IT will ensure access to business information by remote users across public networks is only after successful identification and authentication. Secure channels (such as ipsec, ssl) and technology must be provided for all remote access connections.
- Information security office must regularly inform users on the risks from using mobile computing equipment.

- Appropriate password policy and endpoint security controls must be implemented on all mobile devices.
- A list of all authorized software's installed on the mobile computing devices must be maintained.
- Teleworking must be allowed only after approval from businesses management in conjunction with relevant P&C departments. All necessary controls and recommendations must be provided by Al- Ghurair Group IT based on an assessment of requirements.
- Remote or local access to Al Ghurair information systems or networks must be granted to users only on a need-to-know basis.
- All AGI IT approved removable media must be classified, labelled, handled as per the classification of the highest level of information that it carries.
- AGI IT approved removable media must be securely wiped disposed or destroyed. Only authorized tools must be used for wiping data.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.10.7.1 Management of Removable media	A.8.3.1 Management of removable media
A.11.7.1 Mobile computing and communication	A.6.2.1 Mobile device policy
A.11.7.2 Teleworking	A.6.2.2 Teleworking
A.9.2.7 Removal of property	A.11.2.5 Removal of assets
A..10.7.2 Disposal of Media	A.8.3.2 Disposal of media

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
IPSEC	Internet Protocol Security
SSL	Secure Socket Layer

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 15:48:17 +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 11:17:16 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:22:58 +04'00'

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