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 ensure that backup of business-critical information, applications and systems is available.

3.1 Policy Statements

3.1.1 Data Backup

- All Group's business information, applications and information systems must be backed up.
- Group IT will define the type (full, incremental, or differential) and frequency of backups depending on the business and security requirements of the information involved.
- Availability and recovery of data at rest on workstations and laptops cannot be assured unless this data is backed up by the respective users on to a central storage provided to them. The central storage must be structured and categorized based on the Information Classification policy. Users must be provided with such automated or manual facilities to store all business-critical information.
- The users should avoid storing any critical data on the laptops or desktops. Data encryption mechanisms should be used on mobile devices as an additional control.
- Users should not store personal, non-business-related data on AGI's file servers and central storage systems. All line managers must ensure that the users are informed and educated on the usage of central storage.
- The retention period of all backed up data must be identified by the business after considering all local laws and regulatory requirements specific to the business unit.
- Our organization's backup retention policy is to retain backups for a period of one year.
- AGI IT will ensure that the backup procedures defined are in line with the Business Continuity Plan.

3.1.2 Labelling And Handling of Backup Tapes

- Uniform labelling convention must be used for labelling backup media.
- Based on classification and criticality, backup tapes must be moved to an offsite location at a predefined interval.
- All backup equipment and tapes must be given adequate physical protection i.e. locked fireproof cabinets, both on offsite and on-site locations.
- For the data classified as 'Confidential' the back-ups will be protected by means of suitable encryption or additional logical or physical protection mechanisms.
- Data in transit must be physically and logically protected using adequate controls such as; using trusted couriers or group staff; using locked containers that withstand forced entry; logging and checking of

all dispatch and receipt acknowledgements.

- Movement of all tapes must be recorded and verified by the data center personnel.
- All data backup media must be securely disposed or destroyed. Only authorized tools must be used for wiping data. Relevant approvals from business heads and Group Internal Audit must be obtained before conducting decommissioning any backup media.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.10.5.1 Information backup	A.12.3.1 Information backup
A. 10.8.3 Physical media in transit	A.8.3.3 Physical media transfer

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 15:39:17 +04'00'
Reviewed By	Tabrez Sheikh	Senior Vice President - IT PMO& Governance	Oct 2023	
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 17:26:49 +04'00'

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