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 counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

3.1 Policy Statements

3.1.1 Business Continuity Development

- Each business unit within Group must identify critical functions and ensure that the business continuity plans are addressed.
- Each business must ensure that a managed process exists to facilitate effective development, maintenance, testing and execution of business continuity plans.
- Each business unit within AGI must ensure that a business impact analysis is carried out once in three years, or when major changes to the business occur, in order to determine the potential impact of the interruptions and ensure that alternate controls and processes are put in place.
- Every group company must have a Business Continuity Plan in place which must be reviewed annually or on duration prescribed by any local regulatory, compliance requirements.
- The Business Continuity Planning Framework must be defined to maintain or restore business operations in the required time frames to cause least disruptions to business.

3.1.2 Testing Business Continuity Plans

- A business continuity framework must be designed that states the conditions for activation and personnel responsible for execution of each component of the plan.
- Each business must regularly test the plans to ensure that they are effective and up to date.
- Records of the business continuity tests must be maintained and reviewed by the Information Security, Business heads.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.14.1.1 Including information security in the business continuity management process	A.17.1.1 Planning information security continuity

A.14.1.2 Business continuity and risk assessment	
A.14.1.3 Developing and implementing continuity plans including information security	
A.14.1.4 Business continuity planning framework	
A.14.1.5 Testing, maintaining, and re-assessing business continuity plans	A.17.1.3 Verify, review, and evaluate information security continuity

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 15:50:35 +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 11:21:31 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:20:02 +04'00'

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