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 the logging and detection of unauthorized activities in the information processing infrastructure and systems.

3.1 Policy Statements

3.1.1 Parameters For Logging

- All Business units must be asked to define data access or process logging requirements at the time of system design.
- Logs that are generated must be reviewed at regular intervals. Compensatory controls such as reconciliation reports should be used where complete log review may be resource and cost intensive. Other compensatory controls could include automated disconnection of detected unauthorized activity.
- System administrator and system operator activities must be logged (e.g. the time at which the event occurred, the information of the event or failure, account information, and administrator / operator details etc.).

3.1.2 Log Retention and Its Protection

- All audit logs recording exceptions and other security-relevant events must be produced for critical systems and kept for an agreed period to assist in future investigations and monitoring.
- Controls must be implemented to protect logging facilities and log information against tampering and unauthorized access.
- All logs and records must be maintained on the system. In case of capacity restrictions, logs must be archived and stored via retrievable methods. Logs must not be deleted without verifying the retention requirements from Business, Group Internal Audit, and Information Security.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.10.10.1 Audit logging	A.12.4.1 Event logging

A.10.10.2 Monitoring system use	
A.10.10.3 Protection of log information	A.12.4.2 Protection of log information
A.10.10.4 Administrator and operator logs	A.12.4.3 Administrator and operator logs
A.10.10.5 Fault logging	

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 15:36:43 +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 11:13:30 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.15 12:01:59 +04'00'

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