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 security perimeters for the data processing and computing facilities are defined to prevent unauthorized access, damage, and interference.

3.1 Policy Statements

3.1.1 Physical Security Perimeter

- The security perimeter for the data centers and server rooms must be defined to form a physical boundary.
- All entrances and exits to such premises must be manned 24x7 and will have appropriate two factor electronic access control systems.
- All entrances / exits of data center must be monitored though closed-circuit television systems.
- All racks hosting network or server equipment outside the data center and server rooms must have adequate control for restricted physical access.

3.1.2 Physical Entry Access Controls

- Access to these premises must be restricted to authorized employees of the Group IT Department or those approved by Heads of Group IT.
- External party personnel entry must be allowed only after prior authorization. All visits should be scheduled, and all relevant access control staff must be informed in advance. Visitors to data centers must be escorted throughout their stay. Logs of all entries and exits must be maintained.
- Visitors must be asked to declare their belongings while entering the data centers and this must be verified when the visitors exit.
- All personnel's entering data centers must be required to wear a visible identification. A visible differentiation identification tags must be maintained for external parties.
- A list of personnel's having access to data centers must be maintained. Access rights must be reviewed on a quarterly basis.
- Access points such as delivery and loading areas and other points where public may enter the premises must be controlled and, if possible, physically isolated from information processing facilities to avoid unauthorized access.

3.1.3 External And Environmental Security

- Fire doors must be alarmed, monitored, and tested regularly.
- Fire-fighting systems must be appropriately placed, and maintenance of all equipment must be done regularly.
- Fire-fighting mock drills must be conducted at least once every year.
- Backup media must be stored at a safe distance from the main site.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.9.1.1 Physical security perimeter	A.11.1.1 Physical security perimeter
A.9.1.2 Physical entry controls	A.11.1.2 Physical entry controls
A.9.1.3 Securing offices, rooms, and facilities	A.11.1.3 Securing offices, rooms and facilities
A.9.1.4 Protecting against external and environmental threats	A.11.1.4 Protecting against external and environmental threats
A.9.1.5 Working in secure areas	A.11.1.5 Working in secure areas
A.9.1.6 Public access, delivery and loading areas	A.11.1.6 Delivery and loading areas

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 15:51:21 +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 11:22:25 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:21:19 +04'00'

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