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 security of information in networks and supporting infrastructure of AGI.

3.1 Policy Statements

3.1.1 Network Controls

- Group IT will ensure that the use of network services is consistent with the user access management policy and the requirements of the business applications.
- All business units must use Group's standard network and security devices. The network designs and cabling across the Group will be consistent and in line with Group's requirements for network management, control, and monitoring.
- Business units must ensure that plans for new facilities or business premises should provision secure facilities to host systems equipment.
- Users must not connect any personal, unauthorized network enabled devices to the Al- Ghurair corporate network. This includes, but is not limited to, wireless, Bluetooth hubs, routers, switches, mobile phones, or tablets.
- BYOD (Bring Your Own Devices) such as laptops, computers, mobile devices, hard drives, iPads, etc. should not be allowed to connect to AGI internal network.
- Users must not be allowed to dial to an ISP using their desktop / laptop while still connected to corporate network.
- Group IT will ensure that the numbers of entry points into the network are restricted. All Internet facing entry points must be protected by next generation firewalls (NGFW).

3.1.2 Segregation In Networks

- Network address translation must be used wherever possible to prevent propagation of routes from the internal network to other networks.
- Third party site connections must be terminated securely on a firewall. All third-party connections must undergo a risk assessment in line with the third-party service management policy.
- Servers supporting critical applications must be logically separated from other servers. All servers facing the internet must be installed in demarcated DMZ's (de militarized zones) such as web DMZ, application DMZ, database DMZ and internal DMZ.
- Appropriate technology must be used to maintain the confidentiality and integrity of data passing over public networks such as the Internet or over wireless networks.
- The network and security components used for communication over the network must be appropriately configured, maintained, and secured.

3.1.3 Logging Of Network Devices

- Secure connecting mechanisms must be provided for users to connect to the corporate network while working offsite.
- Logging must be enabled on all network equipment that supports logging.
- Network equipment and supporting utilities must be placed in secluded secured areas (i.e., server rooms or locked, inaccessible cabinets.). Network cables must be concealed or protected from unauthorized interception, especially in public areas.
- Logon banners must be implemented on all network devices to provide warning against unauthorized logon attempts.
- All changes to network devices will follow the change control procedures.
- Network team will maintain relevant network management reports and audit trails for a predefined duration.
- Key network activities will be monitored to assess the performance of the network, reduce the likelihood of network overload, and detect potential or actual malicious intrusions.
- Annual independent penetration tests and network reviews must be conducted to ascertain the security of network and systems security.
- Clocks of all relevant information processing systems within an organization or security domain must be synchronized with an agreed accurate time source.
- The network manager must ensure redundancy at component and service level is maintained to support critical business processes.
- Sufficient technology controls must be implemented while taking network services from a service provider. The controls must consider the confidentiality, integrity and availability of the data being transmitted between the client and the service provider.
- Service Level Agreements must be signed with all network and security service providers.
- Services provided by the service provider must be regularly monitored.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.10.6.1 Network controls	A.13.1.1 Network controls
A.10.6.2 Security of network services	A.13.1.2 Security of network services
A.10.10.6 Clock synchronization	A.12.4.4 Clock synchronization
A.11.4.1 Policy on use of network services	A.9.1.2 Access to networks and network services
A.11.4.2 User authentication for external connections	
A.11.4.3 Equipment identification in networks	
A.11.4.4 Remote diagnostic and configuration port protection	
A.11.4.5 Segregation in networks	13.1.3 Segregation in networks
A.11.4.6 Network connection control	
A.11.4.7 Network routing control	

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
BYOD	Bring Your Own Devices
NGFW	Next generation firewalls
DMZ	De militarized zones

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 15:37:58 +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 11:11:27 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 17:24:45 +04'00'

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