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 access to information and information processing facilities is adequately controlled.

3.1 Policy Statements

- Group IT will ensure that access to information; information processing facilities is controlled based on business requirements and security requirements of individual applications.
- All logon screens for access to systems must include a special notice which must state that the system may only be accessed by authorized users, users who logon represent that they are authorized to do so, unauthorized system usage or abuse is subject to criminal prosecution, and system usage will be monitored and logged.
- Users are not allowed to install any code, software or technique that circumvent the authorized access control mechanisms found in operating systems, application systems or infrastructure system access control mechanisms.
- The IT department must ensure that access is granted only after receiving approvals from respective Information Owners or their representatives from Group P&C
- All new users must be assigned minimum level of privileges. All requests for additional privileges on group multi-user systems or networks must be submitted on a completed system access request form that is authorized by the user's immediate manager, Group P&C.
- All user IDs on Al Ghurair corporate domain computers and networks must follow group user ID construction standard, must clearly indicate the responsible individual's name or employee number. The employee Id field must be included in a dedicated field in all system user databases. Generic Id's must is not used on any system. Service and operating system Id's used internally within systems may have generic or vendor specific names; however, a record of the owner/s of that privilege must be maintained.
- All users must be assigned a single unique user ID for systems and applications. User ID's must is not reassigned after a user terminates their relationship with Group.
- All system administrators must employ at least two different sets of user IDs and passwords. One set is for use as a normal system user and the other to perform system maintenance functions.
- System administrators must not have elevated privileges on their normal user account.
- The computer and communications system privileges of all users, systems, and programs must be restricted based on need to know.

- A formal user registration and de-registration process granting and revoking access to all information systems and services must be in place. This must be in line with Group P&C's procedures for employee on-boarding and termination or reassigning of job roles.
- System administrators must maintain records of all User Access Requests received from the business or Group P&C.
- Business Units must ensure that any change of employee status and access requirements are immediately communicated to Group P&C and Group IT.
- All redundant and dormant user accounts i.e., accounts that have not been used for three months will be disabled.
- Group IT will provide the business units with annual reports of all access privileges to critical systems, process and information. Additional ad-hoc reports can be mandated for systems based on their risk analysis. All business units must ensure that all access privileges are authorized.
- End users will not be given access to invoke operating system, system level commands. They must be restricted to menus that display only those activities which they have been expressly authorized to perform.
- User access rights and privileges shall be reviewed half-yearly or after any significant organizational, systems or personnel changes. Access matrixes shall be maintained at Business unit level and reviewed by Business Owner.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.8.3.3 Removal of access rights	A.9.2.6 Removal or adjustment of access rights
A.11.1.1 Access control policy	A.9.1.1 Access control policy
A. 10.1.3 Segregation of Duties	A.6.1.2 Segregation of duties
A.11.2.1 User registration	A.9.2.1 User registration and de-registration
	A.9.2.2 User access provisioning
A.11.2.2 Privilege management	A.9.2.3 Management of privileged access rights
A.11.2.4 Review of user access rights	A.9.2.5 Review of user access rights

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 15:46:53 +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 11:16:17 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:22:18 +04'00'

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