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

3.1 Third-Party Service Management

The objective of this policy is to ensure the security of information and information systems and software which are accessed by or shared with third parties or any external entity. Third-party refers to contractors, consultants, suppliers, business partners, external auditors, temporary staff, volunteers, and every other type of individual or entity that is not an Al Ghurair employee.

3.2 Policy Statements

3.2.1 Third-Party Agreements

- The business must ensure all third-party engagements that require an exchange of information and access to Information technology systems are reported for a due diligence check to relevant AGI departments, including Group IT, Group Internal Audit, Legal and Group P&C. This can be done by the respective IT customer account managers and customer engagement managers. Business units must review other relevant policies issued by departments, including but not limited to Legal, Human Resources, and Finance.
- AGI must include all relevant security and audit requirements in agreements with third parties (accessing, processing, exchanging, auditing, communicating, or managing the organization's information and information processing facilities).
- In case of requirements that involve integrating Al Ghurair systems with a third-party system, an NDA must be signed with the third-party company at the time of engagement.
- Responsibilities and legal actions for information security breaches must be addressed in the terms and conditions of all agreements with third parties.
- Business unit heads must review relevant Group's policies and consult respective internal departments and ensure copyright and software license compliance during information exchange with outside entities.
- Signed agreements such as non-disclosure must precede the disclosure of sensitive information to external parties. Relevant legal departments must be approached for due diligence on such agreements.
- Security controls, service definitions, and delivery levels included in the third-party service delivery agreements must be implemented and managed by Group and the third parties.
- Wherever the business deems a need for high availability, agreements with external parties must address the type of service and level of service that would be provided to ensure business continuity.

3.2.2 Third-Party Access

- Group IT cybersecurity and Group IT departments must collectively assess risks that are associated with sharing of systems, information, and assets via a formal risk assessment.
- The business line units engaging the third party must assess the business need and risks while defining the access levels required (physical and logical) for the external parties.
- Prior to granting access to any information, Group IT must ensure all third-party users are briefed on information security roles and responsibilities by signing the undertaking document.
- Remote or local access to Al Ghurair systems or networks must be granted to external parties only on a need-to-know basis. The access should be given for a fixed duration after approval by Infosec team and the IT department. The duration of the access should be in line with the duration of the engagement and relevant activity undertaken by the third party.
- Systems which are not part of Al Ghurair corporate domain must not be allowed to directly connect to company's corporate internal network.
- Ad-hoc and 24/7 unmonitored connections by third parties to production systems must not be permitted.
- All administrator related access will be provided only via PAM (privilege access management) and all third party or contractor accounts will have MFA enabled by default.
- Group IT department must ensure that sensitive data sent to third parties over communication channels such as the Internet, WAN links, and extranet links are adequately protected from interception and tampering.
- Where large volumes of data, in the form of entire system backups or database dumps, are required to be exchanged with third parties, additional signoff must be requested by the business/information owner. Third parties must employ sufficient security controls to protect such data.
- The engaging Business/Project Managers must ensure that requests are issued to revoke all third-party access at the conclusion of the third-party service term.

3.2.3 Monitor And Review

- The business line representative/head must monitor and review the services, reports, and records provided by external parties at agreed levels. The following parameters may be considered for the same:
  - performance against service levels
  - noncompliance and issues, e.g., against the SLA or security breaches
  - performance reporting following major events.
  - indications of service improvement opportunities
- A re-assessment of the risks must be carried out due to the internal changes or variations to existing service delivery. Security controls must be identified and improved during and after the process of change.
- Wherever necessary, AGI must conduct audits/reviews of third-party services.

3.3 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.6.2.1 Identification of risks related to external parties	A.15.1.1 Information security policy for supplier relationships
A.6.1.5 Confidentiality agreements	A.13.2.4 Confidentiality or non-disclosure agreements

A.6.2.3 Addressing security in third party agreements	A.15.1.2 Addressing security within supplier agreements
A.10.2.1 Service delivery	
A.10.2.2 Monitoring and review of third-party services	A.15.2.1 Monitoring and review of supplier services
A.10.2.3 Managing changes to third party services	A.15.2.2 Managing changes to supplier services
A. 10.8.1 Information exchange policies and procedures	A.13.2.1 Information transfer policies and procedures
A. 10.8.2 Exchange agreements	A.13.2.2 Agreements on information transfer

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
NDA	Non-Disclosure agreement
WAN	Wide Area Network
MFA	Multi Factor Authentication
PAM	Privilege Access Management
NDA	Non-Disclosure Agreement

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 15:52:07 +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 11:24:08 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:20:57 +04'00'

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