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 that 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 AGI group staff members, vendors, consultants 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

This section seeks to ensure that adequate controls are in place for reporting, monitoring security incidents and that timely corrective or preventive actions are taken to minimize impact on information and information systems. A security incident is defined as any incident that violates the group's information security policies or has the potential to cause loss, disruption, or loss of data via malicious or non-malicious activities by users or external entities.

3.1 Policy Statements

3.1.1 Reporting Security Events and Weaknesses

- Al Ghurair IT leverages 24*7*365 SOC (security operations center) services from Trend Micro which covers the automated response against critical & high severity events.
- Group IT systems is configured to trigger security alerts to system & IT Security administrators (or any other designated personnel in IT). Some security incidents may be identified during applications / systems activity reviews. Line managers or users might observe security violations during daily activities.
- All incidents and weaknesses will be reported to the service desk. Incidents that involve confidential, sensitive information or require special handling and investigation will be directly reported to the Group IT Cybersecurity, Group Internal Audit, Group P&C via the line managers. Each of these departments would then include the other relevant departments to initiate the investigations and control of the incident.
- Security incidents include, but are not limited to, the following:
    - A computer virus attacks or intrusion of Al Ghurair internal and external systems.
    - Unauthorized scanning or browsing of networks and systems.
    - Unauthorized access attempts (unauthorized user activity).
    - Group website defacement, compromise of web facing servers and applications and denial of service attempts.
    - Vulnerabilities identified because of a scan (serious software vulnerabilities)
    - Notifications from service providers or external entities of suspicious activity emanating from Al Ghurair network or systems.
    - Notifications from external entities of any suspicious activity related to Al Ghurair domain names, IP addresses or any violation of intellectual property or confidential information.
    - Loss or leakage of online or archived data / records, media, mobile computing devices
    - Access to a computer using another person's User ID

- Unauthorized use of personal hubs, wireless and Bluetooth switches
- Unauthorized attachment of a workstation, personal/illegal software, or hardware to the network
- Intentional entering of false data, unauthorized modification, or deletion of existing data into production systems.
- Introduction of virus-infected diskettes, CD's, DVD's, USB, and any other removable media to the systems
- Unauthorized erasure of data from a hard drive, tape, or other storage system.
- Unauthorized removal of Al Ghurair software and system documentation
- Any email that violates the email policy or the guidelines distributed by the Group IT security.
- Internet usage that violates the Internet usage policies
- Actions that cause excessive or unusual use of resources thus harming normal operation
- Any observation of unusual or malicious activity on the network (usually aimed at obtaining passwords, commercial or personal information).

3.1.2 Action Against Security Incidents

- Investigations and corrective action will be taken be taken according to the severity of incidents.
- In case of high severity instances, immediate action may be required by Group IT – Cybersecurity, system, and network administrators to contain the incident and prevent major business impact. These may include disconnecting a system, or configuration modification. All such actions must follow the emergency change process of the change management procedures.
- Relevant evidence must be collected, retained, and presented to conform to any legal, regulatory, compliance requirements.
- Incidents must be recorded in ITSM for future reference, review, and audit.
- Based on investigations conducted and corrective action taken, an incident may be considered closed.
- All incident response procedure must be in line with the business continuity policy.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.13.1.1 Reporting information security events	A.16.1.2 Reporting information security events
A.13.1.2 Reporting security weaknesses	A.16.1.3 Reporting information security weaknesses
A.13.2.1 Responsibilities and procedures for incident management	A.16.1.1 Responsibilities and procedures
	A.16.1.5 Response to information security incidents
A.13.2.2 Learning from security incidents	A.16.1.6 Learning from information security incidents
A.13.2.3 Collection of evidence	A.16.1.7 Collection of evidence

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
ITSM	IT Service Management
SOC	Security Operations Center

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 15:40:07 +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 11:05:32 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:24:56 +04'00'

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