Antivirus Management Policy

P-AGI-GroupIT-473

Policy Owner: Chief Information Officer

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 detect and protect the organization from the threats of malicious codes.

3.1 Policy Statements

- Group IT will ensure consolidated endpoint protection software is installed and active on every machine. Such a system should provide for protection against viruses, spyware, malware, mobile code, and intrusion attempts. The configuration of the software must be protected to avoid any unauthorized modifications.
- Group IT will ensure immediate, automated, and centrally controlled initiation of definition update on all endpoints in the organization to protect against new risks and threats.
- Virus scans must be scheduled weekly.
- Group IT will review the protection software activity logs periodically, ensure proper functioning of the software and monitor any malicious code incidents.
- Incoming email attachments and internet downloads must be scanned for viruses. If a virus is detected, the protection systems should be configured to automatically contain the threat.
- End users should be updated on various virus threats on an ongoing basis. They must be informed on steps to take in case a suspected virus attacks their system.
- Any files or data obtained from outside in any media must be scanned for virus before being used.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.10.4.1 Controls against malicious code	A.12.2.1 Control against malware
A.10.4.2 Controls against mobile code	

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 15:43:30 +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 11:04:14 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:24:23 +04'00'

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