Asset Management Policy

P-AGI-GroupIT-463

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 identify, classify, maintain, and dispose of Group's Information assets securely. Information is an asset that, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information can exist in many forms-printed, written on paper, stored electronically, and transmitted by electronic or physical means.

3.1. Policy Statements

3.1.1. Inventory

- Group IT will ensure Inventory of all information assets is drawn and maintained with each business line.
- Group IT will ensure that the information asset inventory is updated and reviewed for accuracy and completeness once every year.
- The asset inventory must include the type of asset, owner, location, backup information, license information, and asset sensitivity.
- Information assets must have an identified owner who will be responsible for safeguarding the assets.
- Information owners must maintain a list of all critical assets that have to be recovered to maintain the continuity of business.

3.1.2. Asset Handling and Usage

- Information asset owners must classify, label, and handle information as per the Information Classification Policy.
- The information owners must review the information classification of the asset inventory at least once a year.
- The acceptable usage policy of assets must be a part of the responsible computing agreement signed by all users as part of the onboarding process.
- Acceptable usage policy must be communicated to employees during induction and through various channels such as awareness mailers.
- Individual Businesses must consult the Group IT Security and Legal for any data retention requirements based on regulatory compliance, industry standards or principal mandates.
- Upon employee termination, Group IT will ensure that all company assets in their possession are handed over to IT or P&C or relevant designated employee, and we will conduct a thorough inventory search to ensure that all assets have been returned. If any assets are not returned or are returned in a damaged state, the employee or user will be held responsible for the replacement or repair cost of the asset.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.7.1.1 Inventory of assets	A.8.1.1 Inventory of assets
A.7.1.2Ownership of assets	A.8.1.2 Ownership of assets
A.7.2.1 Classification guidelines	A.8.2.1 Classification of information
A.7.2.2 Information labeling and handling	A.8.2.2 Labelling of information
	A.8.2.3 Handling of assets
A.10.7.3 Information handling procedures	

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 15:50:11 +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 11:21:05 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 11:19:30 +04'00'

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