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 purpose of this policy to define controls to ensure timely / regular patching of identified vulnerabilities in all operating systems and applications to ensure continued security and reliability of applications and related IT systems.

3.1 Policy Statements

3.1.1 Source Verification

- Cybersecurity team and systems administrators must monitor security mailing lists, review vendor notifications and websites for the release of new patches.
- Group IT will ensure that patches are received from trusted sources.

3.1.2 Patch Classification

- Group IT will categorize all received patches according to the below:
  - Critical: Patches related to any widespread vulnerability or security patches rated as "Critical/Urgent" by the vendor shall be rated as "Critical."
  - High: Security Patches rated as "High" or "Important" by the vendor shall be rated as High.
  - Medium: Security Patches rated as "Medium" or "Moderate" by the vendor shall be rated as Medium.
  - Low: Security Patches rated as "low," "Informational," "non-essential" or "not urgent" by the vendor shall be rated as Low.
- The threat level or criticality of patches defined by the vendors must be considered to determine the urgency of deploying the patches.
- Patches must be prioritized and applied in accordance with Patch Management Standards.

3.1.3 Patch Management

- Group IT will ensure that a complete inventory of technology assets, are included in the initiation phase.
- All IT systems (network devices, servers, databases, applications) shall be updated with the latest security patches.
- Patch management tools shall be utilized to download the latest patches wherever technically feasible and automatically.
- Appropriate tools shall be utilized to deploy patches in a multi-vendor environment.

- End-users shall be notified of the rollout of the latest security patches on all IT systems.
- Wherever required, the software vendors' websites shall be referred to determine the availability of patches.
- Patch deployments towards IT systems shall comply with the change management process.
- A monthly report must be sent to AGI IT security summarizing that month's patch management activity. It must include the successful as well as unsuccessful installations.

3.1.4 Patch Deployment Initiate

- Patch implementation communication must be sent to all stakeholders before the implementation Test.
- All patches must be tested before deployment wherever technically feasible. Systems and application administrators must assess the effect of the application of a patch to the overall network and systems prior to its deployment. Patches must be installed in development environments before deploying to production.
- Development environment must be created that reflects the production environment and allows for software compatibility testing.
- Tests must be conducted to validate that the patch does not cause conflicts with coexisting applications on the system.
- All patch tests and updates must be logged and documented.

Deploy

- Patches will be rolled out quarterly as per the deployment schedule approved for AGI IT
- In case of Zero-day vulnerability patches, the patch will be applied as soon as it released officially.
- In case a system cannot be patched within the timeline due to any concerns, the relevant heads of departments must approve the same and initiate necessary mitigating controls after consultation with Information Security.
- Roll back procedures must be maintained to ensure that the application/device is available even if patching fails to avoid business disruption.

Verify

- Post-deployment, the patch installation shall be verified if it is successfully implemented.
- In cases of application servers, application testing shall be performed once the patch is successfully implemented.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.12.6.1 Control of technical vulnerabilities	12.6.1 Management of technical vulnerabilities

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 15:37:26 +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 11:12:33 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 17:25:18 +04'00'

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