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

This policy aims to establish a process to help identify security vulnerabilities on business applications and related IT systems that attackers could exploit to gain unauthorized access, disrupt business operations, leak sensitive data, and provide necessary recommendations to mitigate the same.

3.1 Policy Statements

3.1.1 Asset Discovery

- Group IT Cybersecurity team will run discovery scans on a periodical basis to identify new assets in the network and to ensure configurations.
- Subscribe & monitor the vulnerability alert services provided by the active community groups/vulnerability information trusted sources / authorized vendors.
- Based on the security alerts on vulnerabilities reported from trusted sources / authorized vendors, awareness communication triggered to internal teams on further actions.

3.1.2 Performing Vulnerability Scans

- Information Security team shall scan using licensed VA tools to identify vulnerabilities in the applications and related IT platforms.
- Vulnerability assessment scans shall be performed on the targeted applications and related IT systems during the following stages.
  - New systems: VA (vulnerability assessments) scans shall be performed on all IT systems including but not limited to servers, network devices, etc., before rolling out in a production network.
  - Existing Systems: Periodic VA scans shall be performed per the scheduled calendar and to include the following:
    - Monthly scan: For primary data centres and primary cloud components
    - Quarterly scan: Disaster recovery data center and any assets not covered in the monthly scan.
- Custom source codes developed by the application development team are peer-reviewed internally within the IT team to prevent common coding vulnerabilities.
- Vulnerability assessment scans performed using licensed code scanning tools as part of the Software.
- From the PCI DSS perspective, CDE Scoped assets, including workstations, shall be scanned at defined intervals.
- Rescan should be performed at periodic intervals or when respective stakeholders fix the vulnerabilities to verify the remediating actions have been implemented.

3.1.3 Penetration Testing

- Penetration testing shall be performed on critical business applications and the related IT infrastructure periodically and when significant changes occur in the IT environment.
- The process shall be established to perform testing periodically on targeted assets.
- Penetration testing schedule to be quarterly for both internal and external IPs.

3.1.4 Remediation

- A vulnerability is said to be remediated if all the systems affected by that vulnerability are remediated.
- The following can be considered remediation of either of these measures:
  - Patching the vulnerability
  - Disabling vulnerable functionality
  - Uninstalling vulnerable components
  - Configuration change
- Remediation of all vulnerabilities shall be done as per the remediation cycle defined in the standards (Refer to patch management control standards)
- If remediation cannot be completed within the given timelines, approved compensating controls must be put within the schedules, and the exception process must be followed.
- Appropriate testing shall be conducted before 'Critical' vulnerability remediation.

3.1.5 Reporting

- The InfoSec team will periodically provide various vulnerability assessment reports to the respective asset custodians / IT teams to fix the vulnerabilities.
- Summary of vulnerability assessment status shall be submitted to senior management periodically.

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
VA	Vulnerability Assessment
CDE	Cardholder data environment
PCI	Payment Card Industry
DSS	Data Security Standard

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 15:35:57 +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 11:14:58 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Oct 2023	Divya Bathija Digitally signed by Divya Bathija Date: 2023.12.14 17:25:50 +04'00'

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