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 ensure that adequate password management controls are implemented groupwide.

3.1 Policy Statements

3.1.1 Minimum Standard for Password Protection

- Users must always keep Group system access passwords confidential.
- Passwords must not be shared under any circumstances.
- Systems must be configured such as users are not permitted to use passwords that are same as the username.
- Users must ensure that passwords are not guessable i.e. using only simple dictionary words, names, and simple sequences of numbers or letters on the keyboard.
- Users must ensure that they do not use passwords for Group systems that are the same as passwords used for personal Internet accounts such as Hotmail, yahoo, Gmail, and social networking sites.
- All users must ensure that passwords are not printed, written down or stored in visible or accessible areas.
- Group IT will issue regular material to educate users on the good security practices in the selection and use of passwords.
- Group systems will be configured to ensure that the following minimum password requirements:
    - passwords are alphanumeric.
    - the minimum length be 8 characters.
    - All user ids will be locked after 5 unsuccessful login attempts.
    - the last 3 passwords are not reusable.
    - all passwords must be stored in an encrypted format.
    - user passwords must not be included in any automated log-on processes.
    - passwords are not recorded in audit trails, logs, or service desk records.
    - passwords must not traverse the network in the clear text.
    - all systems must be configured to force users to change **passwords every 60 days**. System and service accounts may have no expiry passwords. A log of all such accounts, their owners, and usage must be maintained.
- Apart from the above minimum standards, additional password restrictions may be applied to applications and systems based on the sensitivity, criticality, and confidentiality of information and transactions.

- Access to all high-level systems administrator passwords must be controlled. All authorized users of the accounts must be identified, and the user must be recorded. All system passwords must be stored electronically or manually with appropriate security controls for access and non-repudiation.

3.1.2 Reset Of Passwords

- All security administrators will ensure that usernames and initial or reset passwords are not sent via the same communication channel. Two separate channels or mechanisms must be used.
- User identity must be verified before resetting user passwords. Critical systems and applications may have additional reset approvals required from line manager or the Finance manager. Alternately, self-service password reset mechanisms can be deployed with appropriate controls for validating user identity.

3.1.3 Vendor Default Passwords

- All industry default, system default and vendor defined passwords must be changed before the system is deployed in the Group IT infrastructure.

3.2 International Standards Organization 27001 Controls Addressed:

ISO 27001:2005	ISO 27001:2013
A.11.2.3 User password management	A.9.2.4 Management of secret authentication information of users
A.11.3.1 Password use	A.9.3.1 Use of secret authentication information
A.11.5.3 Password management system	A.9.4.3 Password management system

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	Feb 2024	Kamran Manzoor Digitally signed by Kamran Manzoor Date: 2024.02.22 12:20:33 +04'00'
Reviewed By	Tabrez Sheikh	Senior Vice President - IT PMO& Governance	Feb 2024	Tabrez Sheikh Digitally signed by Tabrez Sheikh Date: 2024.02.22 12:28:18 +04'00'
Approved By	Divya Bathija	Chief Information Officer	Feb 2024	Divya Bathija Digitally signed by Divya Bathija Date: 2024.03.07 16:19:40 +04'00'

Date	Version	Changed by	Description
Oct 2023	1	Kamran Manzoor Manager – IT Security	1st Version.
Feb 2024	2	Kamran Manzoor Manager – IT Security	Modified password expiry from 30 to 60 days under Section 3.1.1 – Minimum Standard for password protection