OAG Password Policy

POL 39/2020
Version 1/2020

Reference Document/ Relevant Legislation	ITC Password Policy Document
Commencement Date	Date of EMCM Approval 20th February 2020
Review Date	The review date is 12 months after the commencement date and every three years after that.

POLICY STATEMENT

1 Intent

An important aspect of computer security is the safeguarding of personal and confidential information of all individuals and organizations affiliated with the Office of the Auditor General. Properly chosen passwords by office system users will assist in the control of access to systems and data.

1.1 Passwords are a key part of its strategy to make sure only authorized people can access those resources and data.

1.2 The Office of the Auditor General passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Office of the Auditor General's resources. All users, including contractors and vendors with access to Office of the Auditor General systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2 Scope

2.1 This policy applies to:

2.1.1 All staff of the Office of the Auditor General

2.1.2 All vendors and authorized users accessing Office of the Auditor General Systems and applications

2.1.3 All Information Technology (IT) systems or applications managed by the Office that are storing, processing or transmitting information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

3 Objective(s)

The objective of this policy is to define the acceptable standards for password management of the Office of the Auditor General.

4 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

5 Definitions and Acronym

Policy Maker	Auditor-General
Management	Executive Management Committee

5.1 "Account Lockout Duration" refers to a period of time an account cannot be used after the account lockout threshold has been met.

5.2 "Account Lockout Threshold" refers to how many times an incorrect password can be used before account is automatically disabled.

5.3 "Maximum Password Age" refers to the period of time since a password was set before it is required to be changed.

5.4 "Minimum Password Age" refers to the period of time after changing a password before it can be changed again.

5.5 "Minimum Password Length" refers to the smallest quantity of characters a password can contain to be considered valid.

5.6 "Password" is a code, which, when associated with a user account, provides access to an IT system or application, through an authentication mechanism or a login page.

5.7 "Password History" refers to a user's previous passwords for the specified system.

5.8 Privileged Accounts" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include: administrative and super user accounts.

5.9 "Security Tokens" are logical codes or physical items that must be used in conjunction with a password to successfully authenticate to an IT system. Examples of a security token include: physical access passes; codes to be used on doors' physical security keypads; PIN codes to be used on smartphones;

codes generated by "one-time password" device or software (usually used for two-factor authentication).

5.10 "System or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications.

5.11 "Users" are staffs, vendors and authorized persons accessing Office of the Auditor General's IT systems and applications.

6 Guiding Principles – Password Protection

6.1 Users must protect passwords at all times against disclosure or unauthorized use, including when generated, distributed, used and stored.

6.2 Passwords must follow a minimum set of security requirements including password length, complexity, reuse, and age and account lockout after unsuccessful authentication(s).

6.3 Passwords for Privileged Accounts must follow stronger requirements than regular user passwords.

6.4 In addition to the guiding principles above, passwords must be created and managed in accordance with the guidelines contained in Annexure 1.

7 Supporting Documents/References

ITC Services Password
http://www.itc.gov.fj/images/stories/policies/Password_Policy.pdf

8 Supporting Procedures and Guidelines

The guidelines to this policy are attached as Annexure I to this policy. This information will provide the background to the development of the policy should officers need clarification.

RESPONSIBILITIES	
Implementation	IT Support
Compliance	All Staff
Monitoring and Evaluation	IT Support
Development and/or Review	Corporate Services Division
Interpretation and Advice	System Administrator

9 Exceptions to the Policy

9.1 Exceptions to the guiding principles in this policy must be documented and formally approved by the Auditor General.

9.2 Policy exceptions must describe:

9.2.1 The nature of the exception

9.2.2 A reasonable explanation for why the policy exception is required

9.2.3 Any risks created by the policy exception

9.2.4 Evidence of approval by the Deputy Auditor General

10. Inquiries

10.1 Inquiries regarding this policy can be directed to the Deputy Auditor General

PASSWORD POLICY ANNEXURE 1

Password Requirements

1. Password Protection

1.1. All access and security codes such as passwords, Personal Identification Numbers ("PINs") and security tokens are considered as confidential information and must be protected and handled accordingly.

1.2. All passwords must be protected at all times, as follows:

1.2.1. Passwords must be memorized and must not be written down.

1.2.2. Passwords must be fully encrypted when they are stored, processed during authentication, or transferred over the network.

1.2.3. When a user needs a new password, it can be transmitted in clear-text over the phone or by email when it is: • Randomly generated and sent out individually to each user; and • Valid for a unique transaction, or forced to be changed after the first use.

1.2.4. The "Remember This Password" feature in an application (typically within the web browser) must not be used unless the computer is solely used by a single user at all times (i.e. not a shared computer) and its access is protected.

1.2.5. Passwords must be masked when used in an authentication or login window. This includes the system displaying asterisks instead of the actual password characters, as well as the user ensuring no one can read the password as it is entered on the keyboard.

1.3. Passwords used on different systems (i.e. network domain, applications, network devices, and personal passwords) or for different roles and privileges (i.e. regular user, supervisor or administrator) must each be different where possible. Specifically:

1.3.1. The passwords used on Office of the Auditor General systems must be unique and must not be used on any other non-Office of the Auditor General's systems or applications.

1.3.2. Passwords used to authenticate to external applications, where credentials are sent over an external or public network (for example over the Internet) must be different from passwords used on the internal systems and applications.

1.3.3. The passwords of user accounts with system-level privileges, such as administrator accounts, must be unique and must not be used for other non-administrator accounts.

2. Password Lockout

2.1. The Account Lockout Threshold must be 5 consecutive invalid attempts or less

2.2. The Account Lockout Duration must be a minimum of 10 minutes.

3. Password Complexity

3.1. Passwords must combine a minimum length and the use of complex characters, as follows:

3.1.1. User account passwords should be at least 8 characters long and require the use of at least 3 of the following 4 types of characters:

3.1.1.1. Uppercase characters

3.1.1.2. Lowercase characters

3.1.1.3. Numbers

3.1.1.4. Non-alphabetical characters.

3.1.2. Privileged Accounts, and systems or application accounts (accounts not attributed to a physical person) should be at least 15 characters long and require the use of uppercase and lowercase characters, numbers, as well as non-alphabetical characters (such as punctuation characters, Unicode, or non-printable characters).

4. Password Changes

4.1. Service and application account passwords that remain static or cannot be changed regularly (e.g. service accounts that are application code dependent) must be documented and be protected with increased access controls.

4.2. New passwords must not be the same as one of the last 10 previously used, must not be based on old passwords, and must sufficiently differ from previously used passwords by changing a minimum of 4 characters.

4.3. Default vendor accounts and passwords (including “public”, “private”, “guest”, “administrator”, “admin”, “system”, or any account that comes pre-configured with a vendor’s solution, application or product) must be changed where possible, before a new system is implemented in production, or within one month after becoming operational.

4.4. New user account passwords must be set up as one time use only (i.e. after generation of a new account password, or when a user has requested a password reset, the user must be required to select a new password after first authentication to the system).

4.5. A verification of the user’s identity must be performed by the IT section, Help Desk, or designate before granting a new password.

4.6. All passwords associated with a terminated user, including the user’s accounts or any shared accounts with administrative or high-level privileges that this user has been exposed to, or that were known to this user, must be immediately reset.

5. Network Domain Passwords

5.1. This section applies to Microsoft Windows network domain and shared folders, desktops, laptops, tablets, servers, and databases, including for the domain and the local password policies. The following domain policy settings must be enforced, as a minimum:

5.1.1. Password history: 10 last passwords used

5.1.2. Maximum password age: 90 days

5.1.3. Minimum Password age: 1 day

5.1.4. Minimum password length: • 8 characters for regular users • 15 characters for user accounts with privileges, in order to prevent password attacks based on LM hash

5.1.5. Account lockout duration: 10 minutes

5.1.6. Account lockout threshold: 5 attempts

5.1.7. Reset account lockout counter after: 15 minutes

5.2. Enhanced Network Domain Password Program

5.2.1. Violation of the Password Policy will result in disciplinary action from management.

6. Network Devices Passwords

6.1. This section applies to switches, routers, Wi-Fi access points, firewalls, load balancers, security devices, etc. The following minimum settings must be enforced:

6.1.1. Password history: 10 last passwords used

6.1.2. Maximum password age: 60 days

6.1.3. Minimum password length: 12 characters where possible (8 characters minimum)

6.1.4. Password must include complex characters (numbers and upper-case letters):

6.1.6. Account lockout threshold: 5 attempts

7. Application Passwords

7.1. Application passwords must rely on network domain credentials where possible (Windows Integrated Security).

7.2. When credentials used to authenticate to an application or a system are sent over a public network or an external network (such as the Internet), passwords must be different from the passwords used on the internal network. The following minimum settings must be enforced:

7.2.1. Password history: 10 last passwords used

7.2.2. Maximum password age: 60 days

7.2.3. User account passwords: at least 8 characters long and require the use of uppercase and lowercase characters, as well as numbers

7.2.4. User accounts with privileges, and systems or application accounts (accounts not attributed to a physical person): at least 12 characters long and require the use of both uppercase and lowercase characters, numbers, as well as non-alphabetical characters (such as punctuation characters, Unicode, or non-printable characters)

8. Smartphone Pass-codes

8.1 This section applies to smartphones or cellular phones that process professional email or Office of the Auditor General's information. The following minimum requirements must be enforced:

8.1.1. A pass-code is required to access each device

8.1.2. Pass-codes must be at least 6 characters long

8.1.3. New pass-codes must not be the same as one of the last 10 pass-codes used

8.1.4. Access to the device must be locked after 8 unsuccessful pass-codes entries, for a duration of 5 minutes

8.1.5. Biometric authentication (Facial / Fingerprint) is acceptable as an alternative, or in addition to, a pass-code.

9. Other Passwords

9.1 Voicemail Passwords or Voicemail PINs must:

9.1.1. Have a minimum of 6 numeric digits

9.1.2. Not be the same as the 5 previously used pins

9.1.3. Be locked after 3 incorrect attempts, with a 10 minute wait period

9.2 Remote access passwords used when connecting from an external or public network (such as the Internet) must be:

9.2.1. At least 8 characters long and include uppercase and lowercase characters, as well as numbers

9.2.2. Changed every 90 days when two-factor authentication is not used

9.2.3. Used in combination with a second factor token, where possible

9.2.4. Different from the domain password or any other passwords used within OAG, where possible

9.3. Pre-shared keys used to connect to Wi-Fi networks must be:

9.3.1. At least 8 characters long and include both uppercase and lowercase characters

9.3.2. Changed regularly

9.3.3. Unique to each Wi-Fi network, where possible

9.4. Using Microsoft Office passwords, PDF creator tools or Winzip / 7zip (with no encryption) is only acceptable for the protection of non-confidential documents.

10 Review

This policy will be reviewed 12 months after implementation and every 3 years thereafter.

11 Who to Contact About this Policy

Any queries to be directed to the Deputy Auditor General.

12 Approval

This policy becomes effective on the date approved by the Executive Management Committee.

13 Revision/Change Log

Version 1.0	
Policy endorsed by:	Executive Management Committee
Policy approved by:	Auditor-General
Policy effective from:	Date of EMCM Approval
Policy to be reviewed by:	1 year after the policy becomes effective
Policy prepared by:	System Analyst and Network Administrator
Manager responsible for policy:	Manager Corporate Services