PROVANHALL H.A.

PASSWORD POLICY

	INFORMATION
	PHA recognises the requirement for a robust password policy which is appropriately structured, implemented and reviewed.

1	TERMS of REFERENCE
1.1	The Server managed Group Policy controls passwords which are used for domain accounts or local user accounts. The options utilised are as follows.
2	**ENFORCE PASSWORD HISTORY**
2.1	This security setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords. This policy enables administrators to enhance security by ensuring that old passwords are not reused continually. **Default**: • 24 on domain controllers. • 0 on stand-alone servers. **Note** • By default, member computers follow the configuration of their domain controllers. To maintain the effectiveness of the password history, we do not allow passwords to be changed immediately after they were just changed by also enabling the Minimum password age security policy setting
2.2	**Current : 24**
3	**MAXIMUM PASSWORD AGE**
3.1	This security setting determines the period of time (in days) that a password can be used before the system requires the user to change it. Note that the maximum password age is between 1 and 999 days, therefore the minimum password age must be less than the maximum password age.

	Note • It is a security best practice to have passwords expire every 30 to 90 days, depending on your environment. This way, an attacker has a limited amount of time in which to crack a user's password and have access to your network resources.
3.2	Current : 60 days
4	**MINIMUM PASSWORD AGE**
4.1	This security setting determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days, or you can allow changes immediately by setting the number of days to 0. The minimum password age must be less than the maximum password age, unless the maximum password age is set to 0, indicating that passwords will never expire. If the maximum password age is set to 0, the minimum password age can be set to any value between 0 and 998. Configure the minimum password age to be more than 0 if you want “enforce password history” to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favourite. If the password history is set to 0, the user does not have to choose a new password. For this reason, Enforce password history is set to 1 by default.
4.2	**Current : 1 day**
5	**MINIMUM PASSWORD LENGTH**
5.1	This security setting determines the least number of characters that a password for a user account may contain. You can set a value of between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0.
5.2	Current: 12
6	**PASSWORDS MUST MEET COMPLEXITY REQUIREMENTS**

6.1	This security setting determines whether passwords must meet complexity requirements.
	If this policy is enabled, passwords must meet the following minimum requirements when they are changed or created:
	• Not contain significant portions of the user's account name or full name
	• Be at least six characters in length
	• Contain characters from three of the following four categories:
	  ◦ English uppercase characters (A through Z)
	  ◦ English lowercase characters (a through z)

	• Base 10 digits (0 through 9) • Non-alphabetic characters (for example, !, $, #, %) **Important:** Complexity requirements are enforced when passwords are changed or created. **Default**: • Enabled on domain controllers. • Disabled on stand-alone servers.
6.1	**Client choice : enabled**
7	**STORE PASSWORDS USING REVERSIBLE ENCRYPTION**
	This security setting determines whether the operating system stores passwords using reversible encryption. This provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information. This policy is required when using Challenge-Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Services (IAS). It is also required when using Digest Authentication in Internet Information Services (IIS). **Default:** Disabled.
7.2	**Client choice : disabled**
8	**REVIEW & MONITORING**
8.1	The password policy is defined through server group policy management and therefore once implemented requires no user intervention to administer and monitor.
8.2	M2 will review and verify status on this annually each January N.B. If you require the policy to be verified outwith the normal review process to assist with pre-audit preparation this can be carried out on request.

9	**LIST USER NAMES & PASSWORDS**
9.1	We do not keep list of users and passwords even in secure location. The Administrator can reset any password and the existence of a list undermines the group policy control of the password procedure. In addition the frequency of change normally dictates that any list is frequently out of date which would contravene the policy procedures.
9.2	**Client choice : no list**
10	**STAFF PASSWORD PRIVACY**
10.1	Staff are made aware that their system password should be kept private unless evidently reasonable circumstances exist for it to be communicated to other parties. This is included in the staff induction procedure and informal notification of this is made.
10.2	**Client choice : induction handbook and informal notification**
11	**STAFF EXIT POLICY**
	Staff exit procedure includes instruction to IT to initially change the user password and redirect email. Accounts will be deleted at subsequent Active Directory review. **Client choice : noted**

17 January 2018