<< [Organisation] Logo>>

<< Password Policy >>

Version: 1.0
Date

Revision History

Date	Version	Author	Summary of Changes

Approvals

Name	Signature	Title	Issue Date	Version

Contents

Contents

INTRODUCTION

DOCUMENT PURPOSE

Effective implementation of secure passwords is very much reliant on the staff being aware of what constitutes a strong password and understanding how to maintain robust password management procedures.

Adherence to the statements listed in this policy will ensure that staff are aware of correct password usage and will significantly reduce the risk of compromise due to weak passwords or inadequate password management processes.

SCOPE

One of the aims of the [Organisation] is to educate staff to the correct password usage procedures. This document does not extend to the password procedures and processes required for any external 3rd party staff.

POLICY

Below statement must be complied with by all staff.

Policy Statements

No:	Statements
	All passwords must have at least eight characters.

	Passwords must contain characters from at least two of the three following groups: • upper and lower case alphabetic characters • numeric characters • non-alphanumeric characters
	System generated passwords must not be predictable (e.g. by using obvious or sequential seeds).
	Where these polices cannot be adhered to an appropriate risk mitigation plan must be produced and agreed with ICT Team.
	Staff accounts must be locked if the threshold for unsuccessful logon attempts is exceeded. The exact number of attempts will depend on the complexity of the passwords and the sensitivity of the resources being protected by the password. The maximum threshold is six attempts before lockout occurs.
	Accounts locked due to password failure must remain auto-locked for a minimum of 30 minutes or until manual reset by an authorised person.
	Staff passwords must be changed at least every 60 days.
	Administrator passwords must be changed at least every 90 days.
	Staff passwords created/reset by administrators must be expired so that the system prompts them to be changed at first use.
	Staff must be given a maximum of three opportunities to change their password, once the password lifetime has expired, before the account is disabled.
	All systems must store at least the previous four passwords and there must be no re-use of passwords within this password history.
	Password generation algorithms must not be capable of being reverse engineered.
	Passwords must never be ‘hard-coded’ into software code or software configuration unless access to that password is restricted to more privileged staff or that password is encrypted.
	Passwords must be securely stored – passwords must never be stored in clear text. The strength of the securing mechanism must be commensurate with the system being accessed and the privileges of the staff.
	Passwords must not be displayed on screen whilst being entered.
	Staff must be able to request a password change at any time.
	Dictionary words or other obvious passwords (e.g. date of birth, extension number, children’s birth date, names of pets, “1234567”) must not be used.
	All password authentication mechanisms must use encrypted transmission and storage of passwords. This includes any and all Identity Management or Single Sign On systems