**

**MINSTER MEDICAL GROUP**

**Password Policy**

**MINSTER MEDICAL GROUP**

**Minster Medical Centre**

**Parkwood Health Centre**

**Sheppey Healthy Living Centre**

**Tel: 01795 877714 Fax: 01795 877715**

|  |  |
| --- | --- |
| Name | Helen Gaylor |
| Approval Date | 11.02.2020 |
| Review Date | 11.02.2021 |

##

## General

* Passwords **shall** be used to ensure that access to NHS systems, devices and information is controlled and restricted to approved and authorised users only.
* Passwords **shall** be enforced and used on systems and devices under the control of Minster Medical Group
* Passwords **shall** be complex in nature and follow HMG guidance and best practice.

## Password Creation

* Unique passwords **shall** be created, and used by individuals for each system to which they require access (these will be created under the direction of the relevant system administrators as systems **may** have differing requirements).
* As a best practice guide, passwords **should** be created in the following format:
	+ A minimum of 8 characters long.
	+ Not contain a dictionary word of more than 4 characters.
	+ Contain at least two uppercase letters.
	+ Contain at least two lower case letters.
	+ Contain at least 2 numbers.
	+ Contain at least two special characters or non-alphanumeric characters, such as:
		- ! ” £ $ % & \* @.

## Password Security

* All passwords **shall** be protected to the same level as that afforded to the system or information that they provide access to.
* Users **shall** ensure that if passwords are to be written down they **shall** be stored securely within a sealed envelope in a personal lockable storage device within Minster Medical Group office.
* Users **shall** ensure that passwords are not shared with other users. (If there is a business requirement to share a password approval **shall** be obtained from the Minster Medical Group Management).
* Users **shall** ensure that passwords are never revealed to any other persons. This includes system administrators, security staff and management.
* All Local Server Administrator passwords **should** be changed every 90 days.
* If there is any indication that a password has been compromised that password **shall** be changed immediately and reported as a security incident.
* The Local Administrator Account passwords **shall** differ from domain administration.
* Separate login and passwords **shall** be required for administrators to undertake normal day to user functions.
* No passwords **shall** be incorporated in the hard coding of user accounts in application code.

## Password Management

* Systems **shall** be configured to ensure that passwords meet the required criteria (length, complexity, etc.) for that particular system.
* All new or reset passwords **shall** be changed immediately upon 1st log on.
* Systems **should** be configured to force the change of passwords at regular intervals. These intervals **should** be of sufficient frequency to aid security, but not too frequent that this causes problems for users and administrators.
* Systems **shall** be configured to ensure that passwords, if stored, are held in a secure format (i.e. encrypted).
* Systems **shall** be configured to ensure that previously used passwords cannot be reused.
* Systems **shall** be configured to ensure that new passwords are not just a recycled password with the addition of a number of new characters or the changing of a number of characters.
* Systems **shall** be configured to ensure that following the incorrect entering of a password a specified number of times, the account is locked and can only be opened/reset through a system administrator process. This specified number needs to be small enough in order to add a level of security to the system, but not too small that it causes a burden for user and administrator alike.
* Users **shall** ensure that different passwords are allocated and used on different systems (separate passwords for email account and network logons).
* Users **shall** ensure one password is not simply a derivative of another.