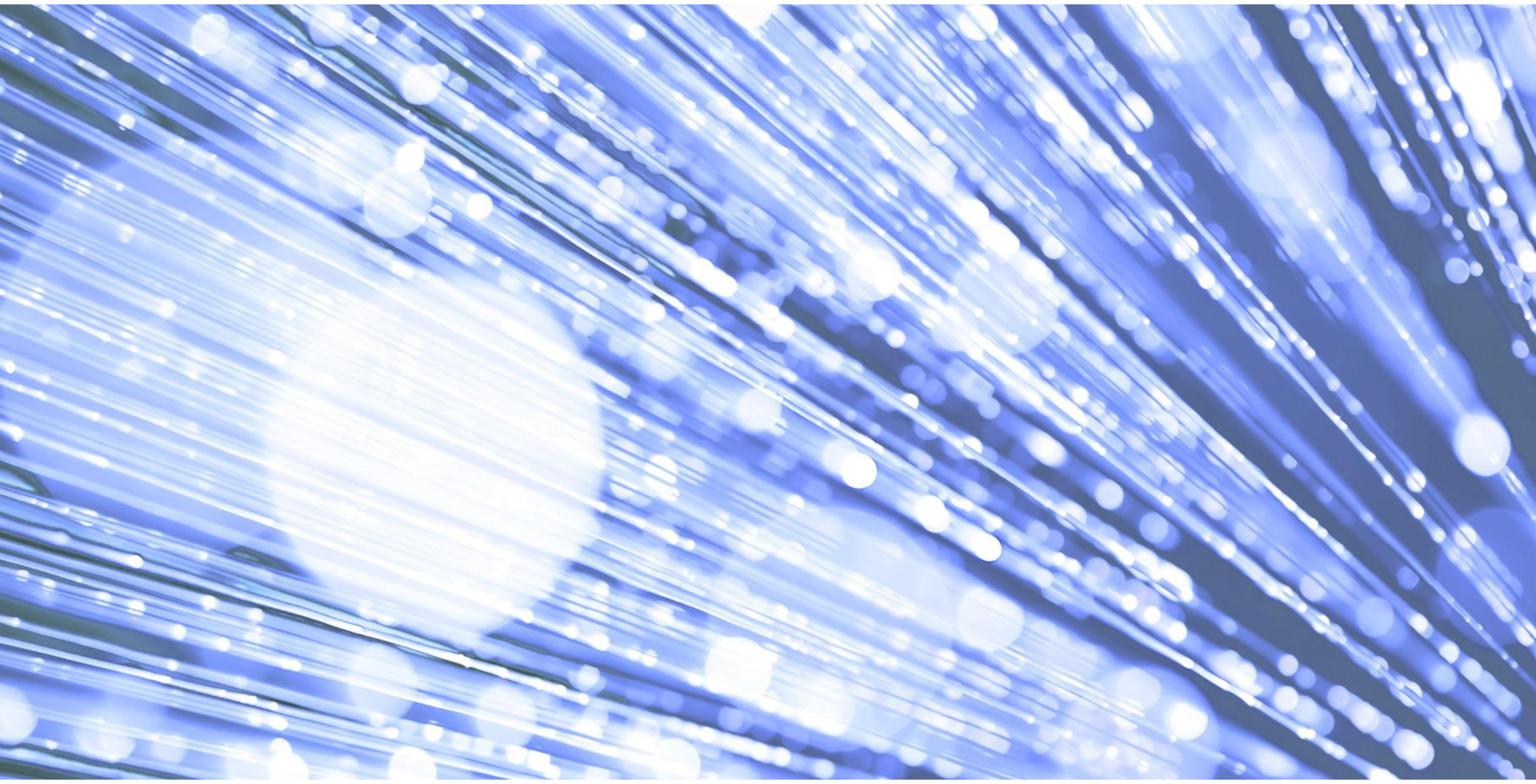
Password

Policy for Ball Tree Surgery

Author: A Heathcote

Date: 24/05/2017

Version: 1.0



Information and technology
for better health and care

Contents

1 Purpose

The purpose of this Password Example Policy is to provide exemplar guidance in line with HMG and private sector best practice for the implementation of an organisation wide Password Policy. This is in order to allow the reader to produce the necessary policies and guidance for their business area and to ensure that the applicable and relevant security controls are set in place in line with the Department for Health, the wider NHS, health and social care and HMG requirements.

2 Scope

The drafting of any policy governing the creation and use of passwords utilised for NHS systems, devices or applications deployed in support of NHS or health and social care business function.

3 Applicability

This Example Policy is applicable to and designed for use by any NHS, health and social care or associated organisations that use or have access to NHS systems and/or information at any level.

4 Guidance

This Example Policy provides guidance on the production of a Password Policy. The Example Policy is in italics with areas for insertion shown as <> and the rationale for each paragraph or section, where required, in [….].

Terminology

Term	***Meaning/Application***
SHALL	*This term is used to state a **Mandatory** requirement of this policy*
SHOULD	*This term is used to state a **Recommended** requirement of this policy*
MAY	*This term is used to state an **Optional** requirement*

Policy

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 Ball Tree Surgery*
- *Passwords **shall** be complex in nature and follow HMG guidance and best practice.*

[Passwords are an easily-implemented, low-cost security measure that will control access to systems, data and electronically stored information if designed and implemented correctly]

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:*
    - *! ” £ $ % & * @.*

[A risk balance will need to be made when deciding on the design and construction of passwords across an organisation. Care should be taken to ensure that complex password requirements do not place an unrealistic demand on users, management and system administrators, while still providing the necessary system access controls.]

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 <insert organisation name> 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 <insert organisation name> 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.*

[An organisation’s passwords are the ‘keys’ to its systems, data and information. Adequate protection must be provided to all passwords and thereby the assets they protect, in order to prevent their loss, compromise or use by unauthorised persons.]

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.*

[The effective management of an organisation’s passwords is essential to ensure that all passwords afford the level of access control they are designed to provide. Organisations should implement a password management regime proportionate to the organisations needs and abilities.]

5 Key Words

Access, Information, Management, Password, Policy