Draft Password Policy

For ORGANISATION NAME

|  |  |
| --- | --- |
| **Policy Group** | Information Governance |
| **Procedure No.** | xx | **Version No.** | xx |
| **Written by** |  | **Ratified By** |  |
| **Date Ratified** |  | **Review Date** |  |

This procedure is applicable to all staff working with ………[organisation name]…………..

**RISK MANAGEMENT STATEMENT**

This policy will ensure the organisation has a consistent, comprehensive and systematic approach to the management of Password Control within the Information Technology systems used.

**1. INTRODUCTION**

The purpose of this Password Policy is to enable the maintenance of integrity across the Organisation’s Information Systems.

This document describes the rules about password maintenance and the standards for the management of access controls in computer based information systems.

**2. PASSWORD DISCLOSURE**

2.1 Staff will ensure that all personal passwords held remain strictly personal to that member of staff and are not disclosed in any form

2.2 They must not be relayed verbally, written down or otherwise revealed to any other individual, either within or outside the Organisation

2.3 If any person accesses information through the use of another person's password, then both individuals may be subject to action in accordance with the Disciplinary policy

2.4 The wilful or negligent disclosure of confidential information whether written or computerised could be seen as a gross misconduct under the Disciplinary Policy and may lead to dismissal

**3. PASSWORD MANAGEMENT**

3.1 Any system capable of using passwords must have the facility enabled

3.2 Length of password and characteristics are system dependent and are therefore are defined

3.3 Passwords should be at least eight characters long and must include a combination of alpha and numeric characters, in any order.

3.4 Passwords must be unique to the system i.e. not be used for access to other systems

3.5 Passwords must not be shared with or disclosed to anyone

3.6 Frequency of password change may be system dependent and passwords must be changed at the frequency defined by the system

3.7 If password change is not system dependent the user should change their password at regular intervals, eg monthly

3.7 Passwords must be changed if security is believed to have been, or actually has been, breached

3.8 Passwords must not be a combination of characters that is likely to be guessed such as a family name, nickname, pet’s name, DOB, car registration or consecutive characters e.g. ABC123

3.9 Passwords must be something memorable so it doesn’t need to be written down. Passwords are encrypted (coded) when applied, and therefore cannot be seen by the system administrators

**4. MANAGEMENT**

4.1 Access to IT systems will only be given once adequate training has been received and competence levels have been reached, as determined by the trainer

4.2 Where systems are locally implemented and maintained and are not under the control of IT or another organisation, training must be carried out by local management

4.3 In the case of PDA’s/laptops and other devices capable of storing or displaying organisational information, (by receiving an email for example) the devices must be protected in line with the ‘Using your own device/Using Mobile data’ Policy

**5. REMOVAL OF SYSTEM ACCESS**

Should there be any breach of this Policy the Organisation may restrict access to any/all systems

**6. BREACH OF POLICY**

All incidents or information pertaining to a potential breach of this policy should be reported in accordance with the appropriate incident reporting policy.

**7. REVIEW OF THIS DOCUMENT**

This document will be subject to review when any of the following occur:

7.1 The adoption of the standards highlights errors and omissions in its content

7.2 When other standards/guidance are suggested which will improve password security and bring it in line with best practice

7.3 2 years elapse after approval of the current version.