Password policy

Created:
Reviewed:

1. Introduction

It is important that security of data held in a central location is supported by a robust password policy to address the risk of unwanted access. This policy forms part of XXXXX's Information Security Policy Framework.

2. Aim

To define a clear password policy to protect the confidentiality of information, protect data integrity, and protect computer systems.

3. Objectives

To protect the organisational resources on the network and systems by requiring strong passwords along with protection of these passwords.

4. Scope

This policy applies to all personnel who have any form of computer account requiring a password on the organisational network including but not limited to a domain account and e-mail account.

5. Policy Framework

5.1. Password Requirements

A number of technical settings have been made which require your password to have a degree of complexity. These are:

5.1.1. Minimum Length - 12 characters
5.1.2. Passwords should use three of four of the following four types of characters: lowercase, uppercase, numbers, special characters (e.g. !"£$%^&*[]{})
5.1.3. Passwords are case sensitive, although remember that your username is NOT case sensitive.
5.1.4. Password history – There will be 12 unique passwords before an old password may be reused.
5.1.5. Minimum password age - 2 days
5.1.6. Account lockout threshold - 4 failed login attempts over 20 minutes
5.1.7. Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. Users must press the CTRL-ALT-DEL keys and select "Lock Computer".

5.2. What constitutes a secure password?

The technical settings from 5.1 are only part of how we select a good password.

It is important that passwords are easy to remember but hard to guess. With password cracking techniques becoming more sophisticated, it's even more important we use more secure passwords.

Examples of bad passwords that are easy for a hacker to guess (using a computer), are: P455w0rd!, Fr33d0m, Password123, Michael1968!, talltrees!23.

The reason these passwords are easier to guess is because they use common words, have simple substitutions of numbers/letters, or have words that go commonly together, i.e. 'tall trees'. To get a more secure password, it needs to be less predictable. Please use these guidelines in choosing a password.

Choose two, unrelated words that do not make sense together. For example:

- Star paws
- Time trees

Add a number at the end or the start (not a birth year or age)

- Star paws 257
- 998 Time trees

Add punctuation and replace some letters with numbers. These are now secure, easy to remember, passwords.

- Star!p4ws257
- 998$Time_tr33s

Finally when creating a password remember that the length of a password is really important to prevent it from being compromised. All passwords should be a minimum of 12 characters.

5.3. Users must not:

5.3.1. Use your XXXXX password for any other purpose, e.g. gmail or personal sites.
5.3.2. Write passwords down.
5.3.3. Send a password through email.
5.3.4. Include a password in a non-password protected stored document.
5.3.5. Tell anyone your password in person or over the phone.
5.3.6. Hint at the format of your password.
5.3.7. Reveal or hint at your password on a form on the internet.
5.3.8. Use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program except for LastPass which is a more secure approach to have this functionality.
5.3.9. Use part of your login name in your password.
5.3.10. Use parts of numbers easily remembered such as phone numbers, social security numbers or street addresses.
5.3.11. Log into their own account in order to allow another user to access it.
5.3.12. Leave your workstation unlocked.

5.4. Users must:

5.4.1. Report any suspicion of your password being broken to the Incident Helpdesk by emailing incidenthelpdesk@XXXXX.co.uk.
5.4.2. If anyone asks for your password, don't give it to them. If they have the ability to reset your password this is a better option than you providing it to them.
5.4.3. Be careful about letting someone see you type your password.

5.5. Resetting of Passwords

Service Desk staff are required to authenticate a user's identity before any passwords can be re-set.

5.6. Documents and databases

It is important that all sensitive information held on files and databases (e.g. excel, word, Access etc) are themselves password protected in a similar manner to the requirements in 4 above.

5.7. Providing Log in Credentials

When creating user accounts for new users or when resetting passwords for existing users it is imperative that the user is provided a complex password and the guidelines above on what to do and what not to do are followed. It is also good practice to ask the user to reset their password when they first login to a complex password that they will remember.

5.8. Other Considerations

Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.

Where available systems should be configured to require two factor authentication and the use of complex passwords.

6. Related Policy and Procedures

6.1. Information Security Policy
6.2. Access Control Policy
6.3. Acceptable Use Policy

Document control

Security classification	
Author	
Owner role	
Approved by	
Approval date	
Distribution	
Signature required	
Latest review date	
Next review date	
References	

Change history

Version	Owner	Changed by	Change summary	Date