UNIVERSITY OF PORTSMOUTH

PASSWORD SECURITY

March 2016

Contents

Document title		
Normal text		
Document author and department		
Normal text		
Approving body		
Normal text		
Date of approval		
Normal text		
Review date		
Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? Tick as appropriate		**YES**
For public access on request copy to be mailed Tick as appropriate	**NO**	**YES**
OR For staff access only (intranet)? Tick as appropriate		**YES**
Password protected Tick as appropriate	**NO**	**YES**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk		

If you need this document in an alternative format, please email corporate.communications@port.ac.uk

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents/qA43279

Summary

What is this document about?

The purpose of this IS Advisory is to present best practice for the creation of strong passwords, the protection of those passwords, and the frequency of change. Strong passwords are critical to computer security and are the first line of defence for user accounts and network access. A poorly chosen password (one that is easy to guess) or one written down and left in open view could cause the entire network to be compromised.

Who is this for?

This advisory is applicable to all University of Portsmouth account holders (inc. Staff, students, third parties and contractors) who have access to, or are responsible for, an account on any University IT system.

How does the University check this is followed?

Annual review of password security will be performed to evaluate the percentage of accounts with weak/unacceptable passwords.

Who can you contact if you have any queries about this document?

Any questions about this advisory should be directed to servicedesk@port.ac.uk

1.0 Introduction

The University must make sure its facilities including IT systems are secure and safe from improper use. All account holders on the University of Portsmouth network and IT systems must follow this IS advisory when selecting their passwords and keeping them secure.

2.0 Best practice:

2.1 **Never give your password to anyone** - not even Information Services staff

2.2 Group account passwords must only be known to named members of the group.

2.3 Passwords should be at least 8 characters long

2.5 Passwords should use characters - drawn from each of the groups below:

- English uppercase characters (A–Z)
- English lowercase characters (a–z)
- Numbers (0–9)
- Non-alphanumeric characters (e.g. !, $, #)

2.6 Passwords should not be a dictionary word in any language (including: slang, jargon etc) or based on personal information, names of family, pets etc.

2.7 Accessing (or attempting to access) another account by deliberately misusing their own or other user's password is an offence under the Computer Misuse Act 1990 and will be considered an act of gross misconduct.

2.8 All system-level passwords (e.g. root, enable, Windows admin, application administration accounts, etc.) should be changed at least every 90 days. Any extension to this period must be approved by the Security Architect.

2.9 If you suspect that your password has been compromised, you must report the matter to the IS Service Desk as soon as possible (ext 7777). IS staff will lock your account and create a fresh password so you can login again. Before doing this, they will ask questions to authenticate who you say you are. If you answer correctly, they will change your password. This authentication step is for your benefit - to stop someone else pretending to be you - and should protect your data and safeguard your privacy – so please be patient.

2.10 Remote access to privileged ('admin') accounts must not be attempted from insecure locations (e.g. open access systems or public terminals).

2.12 Do not use the same password for University of Portsmouth accounts as for other non-University of Portsmouth accounts (e.g. online banking, e-shopping, etc).

2.13 If someone demands that you reveal your password, refer them to this document or have them call someone in the IS Service Desk (ext 7777).

2.14 Writing down your password on a PostIt note and sticking to the monitor or the underside of the keyboard is a very insecure practice.

2.15 Application developers must ensure that their programs (which may use a password mechanism for user access control) also follow these extra security precautions:

- Applications should support authentication of individual users, not groups;
- Applications should not store passwords in clear text or easily reversible format;
- The use of application passwords should be avoided;

3.0 General guidelines on password construction

The primary goal is to create and use 'strong 'passwords - which are easy to remember and difficult to guess.

3.1 Passwords should be resistant to a 'dictionary 'attack (in which a hacker successively tries all the words in a list called a dictionary). Dictionary attacks succeed because many people choose short passwords (7 characters or fewer), such as single words found in dictionaries or simple, predictable variations on words, such as adding digits. (e.g. password123).

3.2 Use a passphrase

A passphrase is generally a longer version of a password and is typically composed of multiple words: The following is a suggested method for creating a strong passphrase:

1. Pick three short unrelated words: e.g. tree, witch, rock
2. Capitalise the first letter of each word: Tree, Witch, Rock
3. Concatenate the words together using a punctuation symbol: Tree?Witch?Rock
4. Add a number Tree?Witch?R0ck

3.3 Use word association

e.g. Amazon - b00ks_&_DVD5 or B00K5//on=line

e.g. PayPal - M@KE-payment5 or is=1T=5AFE?

3.4 Use a song or poem

Mary had a little lamb, it's fleece was white as snow.

This becomes: MHALLIFWWAS or mhall-IFWWA5

4.0 Personal Identification Numbers (PIN)

Certain devices such as phones, door entry systems and mobile devices control access by means of a PIN rather than a password. PINs are normally 4 digits – but they can be made stronger by using more digits – the following best practice rules apply.

4.1 Avoid repetitive patterns: e.g. 0000, 1111, 1122, 4455, 0606, 0707, 0808, 0909

4.2 Avoid predictable number sequences (forward and reverse): e.g. 1234, 9876, 3456,

4.3 Avoid keypad geometry patterns: e.g. 1037, 2486

4.4 The PIN must not contain more than one repeated digit and a repeated digit may not occur more than twice (e.g. 1139 is acceptable but 1122 and 1115 are not).

a. The access PIN for your telephone must not be the same as that phone's extension number.
b. The access PIN must not be based on a year (e.g. *19xx* or *20xx*) or any other well-known date (1066, 1805)

5.0 Enforcement

5.1 Information Services may perform password compliance checks on a periodic basis and inform users if their passwords are found to be weak.

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3141
F: +44 (0)23 9284 3122
E: university.secretary@port.ac.uk
W: www.port.ac.uk