SECURITY WITH PLYMOUTH UNIVERSITY

Technology & Information Services

SEC-GDL-003 - University Account Passwords

Author: Paul Ferrier

Date: 15/02/2018

Document Security Level: **PUBLIC**
Document Version: 1.01
Document Ref: SEC-GDL-003
Document Link:
Review Date: February 2019

SEC-GDL-003 - University Account Passwords

Version	Author	Position	Details	Date/Time
0.9	Paul Ferrier	Enterprise Security Architect	Created the document	10/11/2014 16:50
0.91	Paul Ferrier	Enterprise Security Architect	Updated following comments from Service Management	04/12/2014 16:10
0.92	Paul Ferrier	Enterprise Security Architect	Final amendments following SM feedback	09/12/2014 15:15
1.00	PF	ESA	Updated following change to Password Policy	07/11/2016 14:00
1.01	PF	ESA	Review for 2018	15/02/2018 12:00

SEC-GDL-003 - University Account Passwords

Introduction

These guidelines support the University's Information Security Policy Set and provide assistance into why passwords need to meet the complexity that we require.

Why do we need passwords?

The University has internal systems which records confidential data regarding its staff and students. For example, emergency contact details, home address etc.

The University provides staff and students access to a wealth of informational resources that cost a significant amount of money to subscribe to.

The University plays a major part in worldwide research projects. The information stored and produced may be confidential or sensitive in nature and needs protecting until it is ready to be published.

The information that is categorised as being **Confidential** (not available to the public) or **Restricted** (only available to named users) can be protected in a number of ways, but presently this is performed by the use of an Active Directory (computing account) and an associated password to verify that the user is who they say they are.

Are there any alternatives to passwords?

Yes, there are, but unfortunately, we are not able to implement a solution that provides two factor authentication (something you have and something you are or something you know) at this time, for example the use of a one-time token and a finger print.

Biometrics

Many mobile devices now have the ability to use biometric functions to log you in, for example the university (Toshiba/Levono) laptops all have the ability for users to log in with user defined finger prints; in effect it is substituting the provided password in the background if the finger print matches. This is still a marked improvement on the typing in of a password multiple times a day. This is not an approved University solution at this time and if you choose to use it to log on to your own computer, you do so at your own risk.

The installation of finger print, or smart card readers on all University computing equipment, for example, to sit alongside open access devices would provide a substantial cost to implement; rest assured, the University will continue to provide the most suitable and secured solution for its end users when any change is available.

Why are passwords so complex?

The University is a prime target for ***Phishing attacks***, these are instigated with the intention of acquiring a users' account login and password for malicious use; in addition to this, the account details may be published online for subsequent use. Further information about how to identify a phishing email is available in the SEC-GDL-005-Anatomy of a Phishing Email document. If users don't respond to a phishing email, then there are a number of other methods that a malicious user can undertake in order to break the password of an authorised user. These methods include using the most common passwords disclosed on the Internet or

to use a dictionary attack. This involves a known set of words and repeated loops through the list attempting to use this to access systems coupled with the login ID of the user.

Security audits are carried out periodically and they advise best industry practice surrounding various measures. Using a combination of upper and lower-case letters, numbers and also special characters significantly lengthens the amount of time that is required for a computer to produce the right combination to *crack* a users' password.

Why shouldn't I re-use a password that I've used before?

Imagine if three years ago, you were the victim of a phishing campaign and divulged your University or personal account details. The perpetrator could have placed these credentials onto the Internet, or sold them for profit, either way there will still be a record of this combination of username or email address and password online.

If these details are never used again, they are pointless to anyone that tries to use them, if however, you revert to using them at a later date you are again providing access to your information, to malicious users potentially propagating further attacks or carry out other actions without your knowledge.

Password guidance – How to choose a secure password

Here are some top tips for creating a secure password

Consider using the following:

- **A passphrase**
  Passphrases can use a memorable quote from a film, a book, a song or something similar. For example, "Some people feel the rain, while others get wet" could become "Spftr,w0gW". This is a non-dictionary word and contains the complexity to meet most requirements, including a length of greater than eight characters.
- **Words with character substitutions**
  While this may not be the most secure way of creating a password, it adds a layer of complexity that can still be scripted in a computer program but on the whole, it may deter some malicious users. For example, "Americano" could become "@mer1canO" or "Hot Chocolate" as "H0tch0c0late?". Please note, this is becoming less secure as numeric substitutions are being included in password cracking algorithms now.
- **A password manager**
  There are plenty of password managers out there, that come in either free or low-priced options. The idea behind the application is that you only have to remember one really strong password (as it is protecting the keys to the rest of your kingdom). The applications may often allow you to create really complicated passwords – you won't need to remember.

Things to avoid:

- **Duplicate passwords**
  If your university account were to be compromised, it wouldn't take much to try that password against online banking (or commercial) sites – which may provide a more substantial reward to the malicious user

- **Passwords found online**

  If it is published online, it can easily be incorporated into a malicious software program to try a brute force attack (a method of repeatedly attempting different passwords for a known account) to compromise further accounts

- **Passwords that can be easily guessed**

  The use of dates of birth, family, pet or nicknames and license plates should be avoided, consider who can access, that may be publically accessible that you may have posted on Facebook, LinkedIn, Twitter etc.

- **Keyboard sequences or patterns**

  For example, qwerty, 12345 and asd are some examples that a lot of people will use in their password – because it is easier to remember patterns than complicated passwords

Never:

- **Share your password**

  An extension of number five, even with close colleagues, friends or family, you should never disclose your password to another user. They could write it down or make a note of it – if their account were to subsequently be compromised – your account could be too.

University password requirements

In order to remind you of the current complexity requirements surrounding passwords these are:

Length	Between **9** and **16** characters	**Lowercase**	At least 1 lowercase character (**a-z**)
Numeric	At least 1 numeric character (**0-9**)	**Uppercase**	At least 1 uppercase character (**A-Z**)

Special At least one of twelve approved special characters (**_ $ % ! - ‘ . ^ ( ) { }**)

Finally, don’t use any password in this document – as it is published online.