Password Policy

<table>
<thead>
<tr>
<th>Title</th>
<th>Password Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document ID</td>
<td>Password Policy</td>
</tr>
<tr>
<td>Current Version</td>
<td>1.3</td>
</tr>
<tr>
<td>Sponsor</td>
<td>Nigel Rata</td>
</tr>
<tr>
<td>Author</td>
<td>Dave Cobb</td>
</tr>
<tr>
<td>Date</td>
<td>May 2014</td>
</tr>
</tbody>
</table>

© Copyright Royal Holloway and Bedford New College. The copyright in this document is vested in Royal Holloway and Bedford New College which may also be referred to as Royal Holloway, University of London. The contents of the document must not be reproduced wholly or in part, used or disclosed without prior written permission.
## Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>30/11/11</td>
<td>Draft for review</td>
</tr>
<tr>
<td>1.1</td>
<td>13/02/2013</td>
<td>Annual update and review</td>
</tr>
<tr>
<td>1.2</td>
<td>May 2014</td>
<td>Annual update and review</td>
</tr>
<tr>
<td>1.3</td>
<td>August 2015</td>
<td>Update</td>
</tr>
</tbody>
</table>

## Document Distribution

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nigel Rata</td>
<td>Head of Service Delivery</td>
<td>Document Review</td>
</tr>
<tr>
<td>Sammy Massiah</td>
<td>IT Director</td>
<td>Document Review &amp; Approval</td>
</tr>
<tr>
<td>Judith Crocker</td>
<td>Head of ASD</td>
<td>Document Review</td>
</tr>
<tr>
<td>ITUAG</td>
<td>Various</td>
<td>Document Review &amp; Approval</td>
</tr>
</tbody>
</table>

## Document Approval

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITUAG</td>
<td>May 2014</td>
</tr>
</tbody>
</table>
Contents

Introduction .............................................................................................................................................. 4
Objectives.................................................................................................................................................. 4
Scope....................................................................................................................................................... 4
Password Policy.......................................................................................................................................... 5
Overview................................................................................................................................................ 5
Guidelines ................................................................................................................................................ 5
Construction......................................................................................................................................... 5
Disclosure............................................................................................................................................... 6
Creating and changing passwords ........................................................................................................ 6
Account locking....................................................................................................................................... 6
System and Application administration standards .................................................................................. 6
System and Application procurement and development standards ..................................................... 7
Enforcement ............................................................................................................................................. 8
Exceptions ............................................................................................................................................... 8
Appendices............................................................................................................................................. 8
Appendix I – Password construction tips ............................................................................................. 9
Introduction

Secure passwords, in both construction and safeguarding, are critical elements of digital security. Poorly designed or protected ones can lead to an entire network being compromised and personal data being maliciously accessed. All users at Royal Holloway are expected to abide by the guidelines set out in this policy document.

Objectives

1. Define password standards for end users and system administrators
2. Safeguard user data and data users hold responsibility for
3. Maintain confidence of external organisations in our data safeguarding processes
4. Reduce the possibility and implications of identity theft
5. Avoid unnecessary or complex security procedures by considering the user experience

Scope

This policy is applicable to all users who hold any kind of password authenticated access to any system at Royal Holloway, University of London, on its network or that is otherwise associated with Royal Holloway (such as passwords from systems hosted outside RHUL).
Password Policy

Overview

Passwords are mainly for a user’s personal account only and must not be shared or disclosed to anyone. The scope of this policy also includes system passwords that are non-person specific and relate to roles. It is an offence under the Computer Misuse Act (1990) to access or attempt to gain access to a computer system or material to which one is not entitled. It is also a breach of this policy for any user to misuse their, or another’s, password. If any such misuse results in a user knowingly elevating their system privileges above their assigned level this will be considered an act of gross misconduct.

All user-level and system-level passwords (i.e. basic user, super user, domain administrator) should conform to the guidelines below. In cases where technology prevents this, each exception will be managed and noted on an individual basis. This policy will outline the process by which these exceptions are agreed and managed.

Guidelines

Most users will only have a small number of passwords whilst at Royal Holloway as, strategically; services are implemented with a single-sign-on (SSO) system using a college username and password where possible. Notable exceptions include Turnitin native, MyView (staff payment system) and Upay (the RCS College card top-up system). This makes these guidelines easy to follow for the vast majority of users.

Construction

All passwords must:

• be at least eight characters
• include at least three different types of character from the following
  o uppercase (A-Z)
  o lowercase (a-z)
  o numeric (0-9)
  o special (! @ # £ $ % ^ & * ( ) _ + = | ~ \ ‘ { } [ ] : ; “ < > ? , . / `)

All passwords should:

• not be a word in any language, slang, jargon, etc.
• not be based on personal information (names, fantasy characters, pets, etc.)
• not use computer or Royal Holloway related terms
• not use addresses or phone numbers
• not contain common patterns (e.g. qwerty), repeating patterns (e.g. 12341234) or reflected patterns (e.g. 12344321)
• be based on something memorable
Disclosure

Under no circumstances should any user reveal their password in any way to anyone. Users should never store a password on any computer system unless it is heavily encrypted and ‘remember password’ features should not be used on any shared devices.

If an account or password is suspected to have been compromised, the incident must be reported to the IT Service Desk immediately.

Creating and changing passwords

When a new password is set up by anyone other than the user (typically when it is first created or has been forgotten), wherever possible, the new password will be communicated without anyone else becoming aware of it. Where this is not possible, the user will be required or at least encouraged to change their password immediately.

Users can change their SSO password at any time from a Royal Holloway computer or by visiting passwordmanager.rhul.ac.uk.

Account locking

If more than 20 attempts are made in the space of five minutes to access an account then a ten minute lockout will ensue. The account can be reactivated by contacting the IT Service Desk or waiting for the lockout to expire.

If a user manages to lock themselves out of their account by forgetting the password, the IT Service Desk will only unlock the account once the user has proven their identity.

System and Application administration standards

System and application administrators hold responsibility for implementing this policy and should follow the following additional guidelines wherever possible:

- Password complexity should be enabled to prevent the use of dictionary passwords
- Sharing of system-level accounts should not be used
- If a system provides intruder lockout or break-in evasion features these should be enabled
- Passwords must be stored in an encrypted fashion and password databases protected
- No blank or default passwords are allowed to be used on any system

These administrators include IT Services staff, super users at Royal Holloway and staff with IT responsibility in departments.

1 IT Service Desk: #4321, itservicedesk@rhul.ac.uk, itservicedesk.rhul.ac.uk.
System and Application procurement and development standards

When purchasing or developing systems that rely on password authentication there are a number of minimum standards that must be met:

- Authentication must be for individuals not groups
- Passwords must be stored in an encrypted format
- Provide the capability for role management so one user can subsume the responsibilities of another without their password
Enforcement

Failure to comply with this policy document may result in disciplinary action. Compliance is essential to avoid data theft and unauthorised system access.

Exceptions

Whilst this policy is designed to affect all instances of passwords use at Royal Holloway, there are always exceptions. Users of applications that, for whatever reason, do not conform to these guidelines will be issued with additional information as required.

For systems that wish to be exempt or deviate from this policy - approval must be given by the CIO. The decision and supporting material will by collated with this policy as a record of the process (however these details will not be distributed or published).
Appendices

Appendix I – Password construction tips

Some handy hints for choosing and securing your password:

- Include similar looking substitutions, such as the number zero for the letter 'O' or 'S' for the letter 'S'.
- Include phonetic replacements, such as 'Luv 2 Laf' for 'Love to Laugh'.
- Choose two objects from a picture that you'll always remember. For example: a drawing at your grandparent's house, the illustration from a children's book, a painting at an art museum, etc.
- Choose two terms from a memorable purchase: bluev6 (first car), thinibm (first computer), gold3crt (engagement ring), 7ftgrand (piano), pinedoor (first house).
- Look through a catalogue and choose terms based on something you see.
- Look up a random article on Wikipedia and choose a word found or related to a word you find in the article.
- Separate your two words with symbols and numbers: pine&1&door, kit!2!cat, etc.
- Modify the password for each site: In theory, the most secure password strategy is to use a completely different password for each system. In practice, this means you’ll have to write them down. By choosing a secure password and modifying it based on where it will be used, you can keep a slightly higher level of security. Here are some examples showing how they were created:
  - blue.Mv6 for Amazon.com – blue and v6 from first car. M from the second letter in site name.
  - blue.Av6 for SAP logon – same as above.
  - thin!5!ibm for Amazon.com – thin and ibm from first computer. 5 from the number of letters in the site name.