Credentials Policy

Document Summary

- **Document ID**: Credentials Policy
- **Status**: Approved
- **Information Classification**: Public
- **Document Version**: 1.0 – May 2017
1. Purpose and Scope

The Royal Holloway Credentials Policy informs the University’s staff, students, and other individuals entitled to use University facilities, of the regulations relating to the use of credentials to access IT Services. This policy supports the University’s wider Information Security Policy.

The term “User” refers to any person in receipt of a user ID and/or password issued by the University. These will be references as Royal Holloway Credentials. In addition authentication with hardware tokens, cookies and biometrics etc. may also be classed as credentials.

The consequences of a malicious party gaining access to a computer system using the identity of another person are potentially dire. Everything so accessed including corporate application data, becomes vulnerable to publication, alteration, corruption or deletion.

It is therefore important that all users exercise a duty of care over their user-id and password. This policy informs the users of computer systems what they should and should not do to protect the resources they have access to.

This policy covers all authentication mechanisms for all IT services at Royal Holloway, regardless of whether they are hosted on premise or hosted in 3rd party data centres. This policy also includes access to ‘cloud based’ services where we may be buying software as a service (SaaS). This includes all systems owned and administered by IT Services Staff.

2. Credentials Policy Objectives

2.1 Define credentials standards for all end users and system administrators of College systems
2.2 Safeguard user data and data users hold responsibility for, ensuring College reputation is not unduly at risk
2.3 Maintain confidence of external organisations in our data safeguarding processes
2.4 Reduce the possibility and implications of identity theft
2.5 Avoid unnecessary or complex security procedures by considering the user experience
2.6 Employ best practise/industry standards to ensure audit compliance
3. **Credentials Policy Principles**

3.1 Keep the number of different credentials required to conduct College business to a minimum. This is not meant to encourage reuse of the same credential in multiple systems/services.

3.2 Deploy Single Sign On services (SSO) where possible.

3.3 All new systems (from December 2015) should use Active Directory credentials and enable standard College credentials to be used to admit users into new services.

3.4 All legacy systems should be considered in scope for an authentication health check and reconfiguration during the application/service lifecycle of upgrades.

3.5 This policy will outline the mechanism for systems to be considered out of scope of this policy.

3.6 Blacklist the most common passwords form being set by users.

3.7 Dormant Accounts – staff accounts that have never been logged onto should be disabled after 1 month and then deleted as per the normal cycle.

3.8 This policy introduces Multi Factor Authentication to Royal Holloway – for clarity – Multi Factor Authentication (MFA) enables College systems to prompt users to supply both a password when logging onto a service plus an additional authentication secret. Usually this is provided by the use of a token or token equivalent (such as a smartphone) to provide time sensitive numbers which only the user has access to at the time of logon. In the event of password theft, a criminal would need to have access to the second factor of authentication to gain access to a system and data.

3.9 A users’ role and what data they can access in College systems will determine the password ruleset that will applied to their account. There are 3 rulesets and are outlined below:
<table>
<thead>
<tr>
<th>User Type</th>
<th>Access to:</th>
<th>Ruleset</th>
</tr>
</thead>
</table>
| Standard User             | Access to their own data, no access to College wide data covered by the Data Protection Act (DPA). Examples include students, academics or professional services staff with no access to sensitive information in Banner, Resource Link or Agresso. | • Password must be at least 8 characters long  
• Must not be single dictionary word  
• Must include a mix of letters, numbers, special characters and capitalisation  
• No requirement to change password on regular basis. |
| Advanced User             | Access to data covered by DPA, or role for example, has access to key College processes such as finance approval, multiple examination papers or sensitive College information. | • Password must be at least 8 characters long  
• Must not be single dictionary word  
• Must include a mix of letters, numbers, special characters and capitalisation  
• Users will use Multi-Factor Authentication with no password change. |
| System Administrator or Super User | Access to a majority of data in an individual or multiple College systems. | • Password must be at least 8 characters long  
• Must not be single dictionary word  
• Must include a mix of letters, numbers, special characters and capitalisation  
• Multi-Factor Authentication is mandatory |
4. **User Credential Principles**

4.1 Users must not share their credentials with anyone. IT services will never ask for your password to be revealed.

4.2 Users must not store Royal Holloway credentials in browser (save my password) or 3rd party password safes.

4.3 Users should protect their passwords and avoid loss of credentials by shoulder surfers.

4.4 Users should not write their password down.

4.5 Users should be aware of phishing emails and not provide their logon credentials to rogue systems/services. In the event that users feel they may have given away their credentials, please follow the advice for compromised accounts at the end of this document. The password should be changed as soon as possible.

5. **Assumptions**

5.1 Excessive changing of passwords can lead to reduced security as users suffer password overload and either use common or a single password on many systems, or write their passwords down, which is poor practice.

5.2 Password changing rules should be appropriate to the level of access associated with the user Account.

5.3 Increased password length provides improved security over complexity rules; a combination of the two provides improved protection.

5.4 2 factor authentication provides improved security above complexity, length and regular changes of user passwords.

5.5 IT services will implement systems that reduce the number of Royal Holloway username and password combinations a user is required to use. This will include implementing services that make use of a single Royal Holloway username and password and where possible drive a strategy of single sign-on to reduce the number of times a password needs to be used within the work day. In some cases users may be required to have multiple usernames depending on what access they require to undertake their job.

5.6 IT services will provide a simple, and easy to use mechanism for users to change their password from a majority of devices on the internet.

5.7 Royal Holloway will provide adequate training and communication around the password policy. There will be a focus on the need to reduce the most
common threat vector of password sharing – human
behaviour and the ability for social engineering to access data illegally.

5.8 All default passwords on devices must be changed before connecting to the
College data network.

5.9 Authentication passwords must be for named individuals not groups

5.10 Passwords in systems must be stored in an encrypted format (See Secure
Build Policy)

5.11 College systems will be designed where possible to provide lockout
mechanisms to protect users’ passwords from being guessed by rogue users
and systems.

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

5.13 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.

6. 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:

6.1 System must integrate with standard user directories or federations at RHUL
(e.g. Active Directory, LDAP, Shibboleth etc.)

6.2 Passwords must be stored in an encrypted format

6.3 Passwords should transit between systems and networks encrypted.

6.4 Provide the capability for role management so one user can subsume the
responsibilities of another without their password

6.5 Authentication must be for individuals and not groups

6.6 User roles should be provisioned by the Royal Holloway Identity
management engine and roles and valid user identities be audited in an
automated way on a regular basis to always ensure the correct users have
access to the correct information. (This element is detailed in the Data
6.7 Device authentication in conjunction with user authentication is acceptable.

6.8 The College will not use NIS (Network Information System) as an authentication source. A NTLM (NT Lan Manager) should be disabled so it cannot be used.

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

7.1 Audit logs of authentication should be stored securely in a SIEM solution.
7.2 Review of authentication logs should automated within a SIEM solution to detect unusual activity relating to accounts and the use of credentials, including geographic location, number of attempts etc.

8. **Exemptions**
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, cannot 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 Strategic IT Board (SIB). The decision and supporting material will by collated for audit purposes.
9. Compliance

Each part of this policy states a requirement to audit access and ensure compliance with the policy. A RACI model should be applied.

Responsible: Technical Service Owner
Accountable: Head of Information Services
Consulted: Data Stewards
Informed: All users

Compliance with this policy will be checked on a regular basis. 3 main methods will be used:

- Password audits will be scheduled, checked and maintained, documented and a clear audit trail maintained of actions taken.
- Annual review of password policy compliance will be checked whilst access audits are undertaken for each service, these will be scheduled and reported.
- Spot checks of systems will be undertaken to ensure ongoing compliance between review dates.
- Proactive checks will be spot checked to ensure compliance with policy.

Compromise

If you think your password may have been compromised, change it as soon as possible. If in doubt please contact IT Service Desk, who will be able to assist you. Remember that under no circumstances (via email, phone or in person) will IT Services ask you to divulge your credentials.

Questions:

If you have any questions on this policy or its execution, please contact:

IT Service Desk
01784 444321
itservicedesk@rhul.ac.uk
itservicedesk.rhul.ac.uk
Related Documents:

- Data Access Control Policy
- Secure Build Policy
Document Control Sheet

Revision History

Date of this revision: May 2017

Date of next revision: May 2018

<table>
<thead>
<tr>
<th>Revision date</th>
<th>Summary of Changes</th>
<th>Changes marked</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2017</td>
<td>Initial Draft</td>
<td>No</td>
</tr>
<tr>
<td>January 2017</td>
<td>Post TSO workshop updates</td>
<td>No</td>
</tr>
<tr>
<td>May 2017</td>
<td>SIB Version – 0.5</td>
<td>No</td>
</tr>
</tbody>
</table>

Approvals

<table>
<thead>
<tr>
<th>Ratified by PRC</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIB Ratification</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Classifications: Public

Status: Approved