Password Policy

Contents

1 Introduction ........................................................................................................... 2
2 Scope .................................................................................................................... 2
3 Policy Statements .................................................................................................. 2
4 Sanctions ............................................................................................................... 3
5 Monitoring ............................................................................................................ 3
6 Exceptions ............................................................................................................ 3
7 Definitions ............................................................................................................. 3
8 Related documents ............................................................................................... 3
9 Related requirements ............................................................................................ 3
10 Revision history .................................................................................................. 4

Ownership  Chief Information Officer
Policy Contact  Information Security Manager
Approval  Information Security Steering Group
Protective Marking  Public
Policy Unique ID  POL0002
Last review date  June 2019
Next review date  June 2021
## 1 Introduction

1.1 A password policy is a set of rules designed to enhance information security by requiring strong passwords by using complex and longer passwords.

1.2 Information security threats are increasing, and Goldsmiths is under constant attack from exploited weak passwords to gain entry to our IT systems.

1.3 Password strength is particularly important where multi factor authentication mechanisms do not exist, as is generally the case at Goldsmiths.

1.4 Resetting your password periodically is currently not enforced, although it is best practice to assist protecting users that are unaware their accounts have been compromised.

## 2 Scope

2.1 This policy applies to all Goldsmiths Campus ID accounts.

## 3 Policy Statements

3.1 Password must not contain username.

3.2 Password must be between 12 and 255 characters long.

3.3 Password must be different from previously used ones.

3.4 Password for your Campus ID must not be utilised in any personal or other Goldsmiths IT system.

3.5 Password must contain characters from the four primary categories, including:

- Uppercase letters
- Lowercase letters
- Numbers
- special characters e.g.! $ # % @ +

3.6 Passwords must be reset immediately after becoming aware of active involvement in a security incident.

3.7 Passwords must not be shared with anyone.

3.8 Passwords should not be written down in any format that anyone else can interpret.
3.9 If a password needs to be stored electronically it must be encrypted according to a standard of AES 256 with a password that meets this policy.

3.10 All passwords should be reset at least every 365 days, if used for IT administration or accessing privileged accounts should be every 180 days.

4 Sanctions

4.1 Non-compliant Goldsmiths user accounts may have their access to Goldsmiths Data and Services disabled until the user changes their password to be compliant with the policy.

5 Monitoring

5.1 Goldsmiths may periodically test users’ password compliance with this policy.

6 Exceptions

6.1 Any system unable to support the policy must be reported to the Information Security Manager to record, investigate and advise on alternative controls.

7 Definitions

AES 256: Advanced Encryption Standard algorithm with 256 bit key length.

8 Related documents

- Information Security Policy
- Email policy
- Academic Manual: IT Services Regulations

9 Related requirements

- Goldsmith’s auditor reports
- Information commissioner's office - [GDPR guidance](#)
## 10 Revision history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Details</th>
<th>Author</th>
<th>Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01/08/16</td>
<td>Reviewed by SMT</td>
<td>David Swayne</td>
<td>Approved</td>
</tr>
<tr>
<td>1.1</td>
<td>07/03/19</td>
<td>Reviewed by ISSG</td>
<td>Peter Hircock</td>
<td>Not approved</td>
</tr>
<tr>
<td>1.1</td>
<td>20/6/19</td>
<td>Reviewed by ISSG</td>
<td>Peter Hircock</td>
<td>Approved</td>
</tr>
</tbody>
</table>