Engineers Academy

Password Policy

Date Adopted: 19th July 2022

1. Policy Outline

This policy outlines the measures taken by Engineers Academy LTD, to ensure the passwords used by students, assessors and administrators meet minimum guidelines and expectations.

This policy also outlines the additional measures in place to prevent unauthorised access of student, assessor and administrator accounts, as well as the steps which should be taken if a suspected password breach occurs.

2. Software Security

The Engineers Academy utilises 3rd party software, which adopt their own password policies (WordPress and Moodle). This 3rd party software is accessed by students for the purpose of purchasing courses and conducting their studies. Assessors and administrators access the software to assess student work and for course management, as well as to maintain student records and communicate with stakeholders (Microsoft Office 365 tools). The points provided below are the minimum requirements for such 3rd party software:

2.1 All passwords must be 8 or more characters and must include a capital letter, a number and a special character, as a minimum.

2.2 Multi-Factor Authentication (MFA) is used for additional security, when accessing Microsoft Office 365 administrative settings.

2.3 10 subsequent incorrect attempts at an account password will result in the account being locked for 5 minutes, as a minimum.

In addition, the following points are strongly advised:

2.4 Identical passwords should not be used for multiple accounts on different services.

2.5 Passwords should not be written down, unless stored in a secure place.

2.6 Password managers should not be used, unless password protected.

3. Hardware Security

In addition to the software password requirements outlined above, Engineers Academy assessors and administrators work from home. It is essential that devices used to access Engineers Academy resources and data, as well as routers and firewalls are configured with unique, strong password protection.

The following terms also apply to firewall passwords, router / hub passwords and any desktops, laptops and mobile devices, used for business purposes:

3.1 All passwords must be 8 or more characters and must include a capital letter, a number and a special character, as a minimum.

3.2 Where PINs are used in place of passwords to access devices, 6 or more digits are required, with 2-factor authentication in place, when accessing business information and data.

3.3 Automatic security updates must be enabled on network equipment and devices.

In addition, the following points are strongly advised:

3.4 Identical passwords should not be used for multiple accounts / services.

3.5 Passwords should not be written down, unless stored in a secure place.

3.6 Password managers should not be used, unless password protected.

4. Suspected Password Breaches

If students, assessors or administrators suspect a password breach, either on 3rd party software as outlined in section 2, or on home office equipment as outlined in section 3, the following action steps must be taken:

4.1 The password subjected to the suspected breach must be changed immediately, following the password rules detailed above.

4.2 The suspected breach must be reported, whereby:

4.2.1 Students must report the breach to an assessor or administrator,

4.2.2 Assessors must report the breach to an administrator or director,

4.2.3 Administrators must report the breach to a director.

4.3 Directors will decide on an appropriate course of action, depending on how and where the breach took place.