Bespoke Professional Development and Training Limited

Information Security Policy

Updated: June 2021
Next renew due: June 2022

Version Number	Last Amended	Amended By-
v1	July 2019	Tracey Carter
v2	July 2020	Tracey Carter
v3	June 2021	Tracey Carter

Background

The continued confidentiality, integrity and availability of information systems underpin the operations of BePro. A failure to secure information systems may jeopardise the ability of BePro to fulfil its mission and have greater long term impact through the consequential risk of financial or reputational loss.

This Information Security Policy provides the guiding principles and responsibilities of all members of BePro required to safeguard its information systems.

Successful implementation will only be possible if all members of BePro are aware of, and carry out, their own personal responsibilities.

Purpose of Policy

The intention of this policy is to:

- Ensure that the information systems that BePro manages are protected from security threats and to mitigate risks that cannot be directly countered.
- Ensure that all members of BePro are aware of and able to comply with relevant UK and EU legislation.
- Ensure that all users are aware of and understand their personal responsibilities to protect the confidentiality and integrity of the data that they access.
- Ensure that all users are aware of and are able to comply with this policy and other supporting policies.
- Safeguard the reputation and business of BePro by ensuring its ability to meets its legal obligations and to protect it from liability or damage through misuse of its IT facilities.
- Ensure timely review of policy and procedure in response to feedback, legislation and other factors to improve ongoing security.

Scope

This Information Systems Security Policy applies to all members of BePro, all third parties who interact with BePro information, and all of the systems used to store or process it.

Awareness and Communication

All individuals can access this policy through BePro's website or on request. Individuals will be informed of their rights when making contact with BePro. Individuals applying to use BePro's services will be directed to the policy at enrolment.

Updates to guidance will be publicised through BePro's website.

Information Security Principles

The following principles provide a framework for the security and management of BePro's information and information systems.

Information should be classified in line with any legislative, regulatory or contractual requirements that might increase the sensitivity of the information and security requirements.

Where personal data are stored, appropriate consent for storage and processing must be gathered and recorded in line with current legislation.

All individuals covered by the scope of this policy must handle information appropriately.

Information should only be available to those with a legitimate and lawful need for access.

Information will be protected against unauthorised access and processing.

Information will be protected against loss and corruption.

Information will be disposed of securely and in a timely manner with measures appropriate for its classification.

Breaches of policy must be reported to BePro by anyone aware of the breach, in a timely manner.

Legal and Regulatory Obligations

BePro and its staff/learners must adhere to all current UK and EU legislation as well as regulatory and contractual requirements. This includes GDPR regulations which came into effect 25 May 2018.

Compliance and Incident Notification

It is vital that all users of information systems at BePro comply with the information security policy. Any breach of information security is a serious matter and could lead to the possible loss of confidentiality, integrity or availability of personal or other confidential data. Such a loss may result in criminal or civil action against BePro and also the loss of business and financial penalties.

Any actual or suspected breach of this policy must be notified to the managers at the earliest possible opportunity. All security incidents will be investigated and consequent actions may follow in line with this policy and relevant laws.

BePro Directors will be informed of any breach found to affect personal data in keeping with BePro's Data Protection Policy. Compliance with this policy should form part of any contract with a third party that may involve access to BePro systems or data.

Responsibilities – Individuals

Individuals must follow relevant procedures and guidance. An individual should only access systems and information they have a legitimate right to and not knowingly attempt to gain illegitimate access to other information. Individuals must not aid or allow access for other individuals in attempts to gain illegitimate access to data. In particular, individuals should adhere to the information security 'dos and don'ts' outlined below.

These responsibilities extend to all equipment used for BePro business, including office computers and personal devices.

DO

Do use a strong password and change it if you think it may have been compromised.

Do report any loss or suspected loss of data.

Do be on your guard for fake emails or phone calls requesting confidential information - report anything suspicious to info@beprodevelopment.co.uk.

Do keep software up to date and use antivirus on all possible devices.

Do be mindful of risks using public Wi-Fi or computers.

Do ensure BePro data is stored exclusively on BePro systems.

Do use the designated secure cloud storage to store documents.

Do password protect and encrypt your personally owned devices.

Do familiarise yourself with and follow the relevant data protection and General Data Protection Regulations (GDPR).

DO NOT

Don't give your password to anyone.

Don't reuse your BePro password for any other account.

Don't open suspicious documents or links.

Don't undermine the security of BePro systems.

Don't provide access to BePro information or systems.

Don't copy or share confidential BePro information or personal data without permission.

Don't use memory sticks or other portable devices; BePro's secure cloud storage should be used.

Don't leave your computers or phones unlocked.

Review

This policy will be reviewed at intervals of 1 year to ensure it remains up to date and compliant with the law.

The policy was last updated June 2021 and is due for review May 2022
The policy may also be reviewed if legislation changes or if monitoring information suggests that policy or practices should be altered.

Georgina Selmi
CEO

Tracey Carter
Head of Quality and Compliance