P4C Associates Ltd., IT Security Policy

Updated: October 2020

This IT security policy helps us:

- Reduce the risk of IT problems
- Plan for problems and deal with them when they happen
- Keep working if something does go wrong
- Protect company, client and employee data
- Keep valuable company information, such as plans and designs, secret
- Meet our legal obligations under the General Data Protection Regulation and other laws
- Meet our professional obligations towards our clients and customers

P4C Associates take information security very seriously especially given the extremely sensitive and personal information we typically are party to. We recognise any deliberate or accidental disclosure of any confidential information has the potential to harm the business and impact on clients and end users. This policy is designed to minimise that risk.

Responsibilities

Rory Fidgeon is the Director with Overall responsibility for IT security strategy and has day to day responsibility for implementing this policy and is the Data protection officer (DPO) tasked with advising on data protection best practices.

Review process

We review this policy on a 6 monthly basis. However, as evolving legislation comes into affect we may choose to review its contents on an ad hoc basis. If you have any questions please contact:

Rory Fidgeon via (+44) 01803 269 776

Information classification

We will only classify information necessary for the completion of our duties. We will also limit access to personal data to only those which need it for processing. We classify information into different categories so that we can ensure that it is protected properly and that we allocate security resources appropriately:

- **Unclassified**. This is information that can be made public without any implications for the company, such as information that is already in the public domain.
- **Employee confidential**. This includes information such as medical records, pay and so on.
- **Company confidential**. Such as contracts, source code, business plans, passwords for critical IT systems, client contact records, accounts etc.
- **Client confidential**. This includes personally identifiable information such as name or address, passwords to client systems, client business plans, new product information, market sensitive information etc.

We purposely seek to limit the amount, duration stored and type of all data held by the organisation to the absolute minimum required by our business.

We recognise the information we keep as follows -

A) Type of information e.g. Customer records
B) Systems involved e.g. Microsoft Office
C) Classification level e.g. Company confidential

We do not protectively mark all documents and systems beyond the psychological reports we professionally create. However, it is assumed all information is confidential unless otherwise noted.

Access Controls

Internally, as far as possible, we operate on a 'need to share' rather than a 'need to know' basis with respect to company confidential information. This means that our bias and intention is to share information to help people do their jobs rather than raise barriers to access needlessly.
As for client information, we operate in compliance with the GDPR 'Right to Access'. This is the right of data subjects to obtain confirmation as to whether we are processing their data, where we are processing it and for what purpose. Further, we shall provide, upon request, a copy of their personal data, free of charge in an electronic format. We also allow data subjects to transmit their own personal data to another controller and have them transmit it to them personally.

However, in general, to protect confidential information we implement the following access controls:

A) Company confidential - only available to DPO
B) Client Confidential - only accessed by those who need to directly use it as part of their work and only shared via secure sub-processors and password protected systems.
C) Employee confidential - only available via DPO

In addition, admin privileges to company systems will be restricted to specific, authorised individuals for the proper performance of their duties e.g. creation of psychological reports.

Security Software
To protect our data, systems, users and customers we use the following systems:

- Laptop and desktop anti-malware e.g. Windows Defender. Norton 360
- Email spam, malware and content filtering via email provider
- Email archiving and continuity again via email provider

If any new employee joins or leaves P4C Associates access will be added (together with appropriate training) or removed from appropriate systems.

We also ask employees to -

- Remove software that they do not use or need from all their computers
- Update the operating system and applications regularly (or when prompted to by provider)
- Keep security programs switched on
- Store files in official company storage locations so that it is backed up properly and available in an emergency.
- Switch on whole disk encryption
- Understand the privacy and security settings on your phone and social media accounts

- Make sure your computer and phone logs out automatically after 15 minutes and requires a password to log back in.

Password Guidelines

- Change default passwords and PINs on computers, phones and all network devices
- Don't share your password with other people or disclose it to anyone else
- Don't write down PINs and passwords next to computers and phones
- Use strong passwords and change them regularly
- Don't use the same password for multiple critical systems

Additionally

- P4C Associates regularly access security awareness updates via the internet through such sites as "Get Safe Online" and GDS's Gov.UK
- Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender.
- Remain on guard against social engineering, such as attempts by outsiders to persuade staff to disclose confidential information, including employee, client or company confidential information to protect from fraudsters and hackers
- Remain wary of fake websites and phishing emails. Don't click on links in emails or social media. Don't disclose passwords and other confidential information unless you are sure you are on a legitimate website.
- Ensure we use social media, including personal blogs, in a professional and responsible way, without violating company policies or disclosing confidential information.
- Take particular care of computers and mobile devices when we are away from home or out of the office.
- Ensure those leaving the company, return any company property, transfer any company work-related files back to the company and delete all confidential information from systems as soon as is practicable.
- Where confidential information is stored on paper, it is kept in a secure place where unauthorised people cannot see it and destroyed when no longer required.
- Also the following things (among others) are, in general, prohibited on company systems and while carrying out your duties for the company and may result in disciplinary action:

A) Anything that contradicts our equality and diversity policy, including harassment.
B) Circumventing user authentication or security of any system, network or account.
C) Downloading or installing pirated software.
D) Disclosure of confidential information at any time.

Back-up, disaster recovery and continuity

- All documents, files, and business critical systems are backed-up to two separate and physically differentially distinct hard drives that are solely used for this purpose. This is done on a monthly basis.
- All emails are held by our email provider on their password protected system and hardware
- All psychological reports are held by external test providers and NOT by P4C Associates
- During times of severe disruption all staff can access systems and information via mobile devices – this is tested continuously
- As required under the GDPR, where a data breach is likely to result in a 'risk' for the rights and freedoms of individuals' we must notify the customers and data controllers 'without undue delay'. We will ensure we inform them within 72 hours.

Any additional information regarding security issues may be obtained by contacting: Rory Fidegon as DPO on (+44) 01803 269 776