GDPR Information Security Policy

Who We Are (The Company)

APG Cover is a trading style of Future 45 Limited (The Company)

ADDRESS ..... The Business & Technology Centre, Stevenage SG1 2DX
COMPANY REGISTRATION No 5407413
DATA PROTECTION REGISTER No. Z933878X
FINANCIAL CONDUCT AUTHORITY (FCA) No. 461102
0208 543 6006
email@apgcover.co.uk

Purpose

To ensure that information stored and processed by The Company, or on behalf of The Company, in any form and any location, is securely protected against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that The Company maintains. This policy also addresses the people that use them, the processes they follow, and the physical computer equipment used to access them to ensure that high confidentiality, quality and availability standards of information are maintained.

Scope

This Information Protection Policy applies to all the systems, people and business processes that make up The Company's information systems. This includes all employees, contractual third parties and agents of The Company who have access to our Information Systems or information used for Protect4Sure purposes

Definition

This policy should be applied whenever Business Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Speech.

Risks

We recognise there are risks associated with users accessing and handling information in order to conduct official business.
This policy aims to mitigate the risks including but not limited to: -

- the non-reporting of information security incidents
- inadequate destruction of data
- the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of The Company and may result in financial loss and an inability to provide necessary services to our customers.

Policy Compliance

If any user is found to have breached this policy, they may be subject to our disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
If you do not understand the implications of this policy or how it may apply to you, seek advice from the Data Protection Officer.

Responsibilities

The Data Protection Officer is responsible for ensuring that appropriate information security processes are implemented. Risk assessments will be undertaken to identify the probability and impact of security failures and to determine the appropriate security measures to be applied to information.

This policy and specific subsidiary information security policies, standards and arrangements issued to support it will be regularly reviewed and audited.
Monitoring, enforcement and (where necessary) interception will be used to ensure compliance with The Company's information security policies.

Subsidiary Information Security Policies And Standards

The Protect4Sure GDPR Security Policies consists of a number of documents which must be followed to protect all information The Company holds, as well as our IT systems.

Key Messages

- The Company maintain inventories of all important information assets.
- All information assets, where appropriate, are assessed and classified by The Company.
- Users are not allowed to access personal data until The DPO is satisfied they understand and agree the legislated responsibilities for the information that they will be handling.
- Personal data information must not be disclosed to any other person or organisation via any insecure methods including paper-based methods, fax and telephone.
- Disclosing personal data information to any external organisation is also prohibited.
- The disclosure of such classified information is a disciplinary offence.

More Information

If you're looking for more information, please let us know by contacting our Data Protection officer by telephone, email or post. All contact details are available at the top of this document.