GPS GENERAL PRACTICE SOLUTIONS
EXPERTLY NAVIGATING SUCCESS

71-75 Shelton Street, London, WC2H 9JQ | www.generalpracticesolutions.net
020 8865 1942 | enquiries@generalpracticesolutions.net

CYBER SECURITY POLICY

INTRODUCTION

This policy is to ensure GPS workers applies Information Governance guidelines on cyber security, including implementing a robust defence against and reporting attempted cyber-attacks, and being aware of the dangers of systems being infected by malicious software (malware). These measures are put in place to protect information assets, such as the records of client provider and their service users.

CYBER ATTACKS

Cyber-attacks are an increasing threat, in terms of their growing sophistication and the scale of the detrimental impact they can cause. One of the main methods for such an attack is the sending of unsolicited emails that have been specifically designed to trick users into clicking links or opening attachments that will result in malware being downloaded to their system. GPS will guard against weaknesses in system configurations and promote working practices that guard against cyber-attacks.

MALWARE

Malware is commonly defined as any software that is hostile or intrusive, and includes computer viruses, worms, Trojan horses, ransomware, spyware, adware and other malicious programs.

GPS sets out the following controls to address the risk posed by malware in terms of reduced integrity and availability of its information assets:

- All software installed on organisational assets is to be appropriately licensed.
- The IT directorate at GPS must authorise any installation of software.
- The IT directorate at GPS is responsible for the installation and regular update of anti-virus software on all appropriate machines (servers and clients).
- All media is to be virus-checked before being used.
- Procedures for reporting and handling virus attacks and recovering from them to be implemented, including immediate reporting of any suspicion of virus.

Workers being made aware of the above controls, and the responsibilities arising from them, is of primary importance to the GPS. Workers remaining vigilant to the threats of malware is essential in ensuring that only licensed software is used and that suspicious email attachments are dealt with appropriately.

DEALING WITH CYBER ATTACKS

In the event of a cyber-attack, GPS will limit the damage caused by an attack and reduce the time it will take to recover, as well as the costs involved, by having plans in place to:

- Isolate the incident.
- Make timely and effective repairs to hardware and systems where necessary.
- Recover any data that has been compromised.

PASSWORD MANAGEMENT

Passwords should be strong and secure, changed on a regular basis and not shared with others. Passwords used for personal email accounts etc. should not be the same as ones used for GPS-based accounts. Where it is suspected that a password has been compromised, it should be changed immediately.

REPORTING SERIOUS INCIDENTS

All incidents will be investigated immediately and reported using the Significant Incident procedure in a timescale appropriate to the initial risk assessment. Reports and recommendations will be approved and monitored by the GPS's Information Governance Lead, who will escalate as appropriate.