Policy No: 03-1518	Authorised: Pellagia Margolis	Date: 15/01/2020

CYBERSECURITY POLICY
(GDPR)

`

The Organisation considers that good cybersecurity crosses over a number of management policies – it is not just a matter of putting in place an information security policy. Consequently, the Organisation will address key issues which are set out in this Policy in check-list format, and they will be implemented where appropriate across the entire suite of internal Policies, Record Forms and Worksheets, and Policy Training Questionnaires:

POLICY IMPLEMENTATION:

1. Management and Administration:

1.1 Policies are checked, updated on a regular basis, and enforced.

1.2 There is a nominated staff member with special responsibility for cybersecurity.

1.3 The nominated person responsible for cybersecurity meets regularly with the Domiciliary Care senior staff.

1.4 The nominated person has clear responsibility for cybersecurity, with clear reporting lines and decision-making authority.

1.5 The physical security of appropriate premises is ensured.

1.6 The Organisation allocates sufficient budget to ensure the safe and effective management of cybersecurity.

1.7 The Organisation subscribes to cybersecurity updates to ensure it remains aware of new and existing threats.

1.8 There is an effective data breach response plan, which is validated and updated regularly (reference *Policy No: 1516*).

1.9 There is appropriate cyber-liability insurance in place.

2. Staff:

2.1 There are appropriate procedures in place for staff to be able to report suspicious e-mails quickly and effectively.

2.2 Staff training includes an awareness of cybersecurity.

2.3 Staff knowledge is challenged, for example, by sending spoof phishing emails.

2.4 Staff undertake reviews to ensure that they understand cybersecurity risks, and results checked to ensure improvement.

2.5 Staff understand the risks associated with using public wifi.

3. Hardware, Data Encryption and Technology:

3.1 Backup data is encrypted.

3.2 Procedures provide for sending files securely.

3.3 There is an Approved List of servers, and the individuals responsible for ensuring that they are kept up to date.

3.4 Appropriate firewalls and intrusion detection software are installed.

3.5 Test servers are appropriately configured, and only contain dummy data.

3.6 Wireless networks are appropriately secured.

3.7 E-mail and internet traffic filtering software is installed as appropriate.

3.8 Procedures provide for the review of unsuccessful attacks and probes / scans.

3.9 IT Hardware and software are included on asset inventory lists.

3.10 There is an Asset Management Policy.

3.11 Data is classified according to sensitivity and risk.

3.12 Procedures provide for appropriately limited access to data.

3.13 Data is effectively encrypted.

3.14 Data is effectively backed-up on a regular basis.

3.15 There is an appropriate Patching Policy which is applied consistently.

3.16 Where automated patching software is used, periodic checks are conducted to ensure that it is operating properly.

3.17 There are appropriate configuration management systems in place.

3.18 Anti-virus software is loaded and activated on users' devices at all times.

3.19 Log files are retained for at least a year.

3.20 Automated analytics are used on log files.

3.21 There are appropriate Policies in place regarding the use of external hard drives or USB / "flash" drives.

4. Third Party Risks:

4.1 Staff understand risks arising from third party service providers.

4.2 Appropriate due diligence is undertaken before engaging third party service providers.

4.3 Third parties are assessed for cybersecurity risk.

4.4 There are appropriate contractual obligations on third parties to take steps to keep data secure.

4.5 Where cloud storage is used there are appropriate contractual requirements to be notified quickly of potential security issues.

FORMS REFERENCES:

Form No: 1-505 *Risk Assessment* – Cybersecurity