Southern Hampshire
PRIMARY CARE ALLIANCE

Cyber Security Policy

1.1

Document Type:	Policy & Procedure/Protocol/etc
Current Status:	NEW
Version:	1.1
Reviewed by:	Lee Busher
Latest review date:	July 2022
Original author:	Susan Williams (via FPM)
This version approved:	01/02/2021
Next review due:	July 2024
Approved by	Dr Kirstine Haslehurst
Original publication date	01/02/2021
Applies to:	e.g. All Southern Hampshire Primary Care Alliance Staff/Clinical Staff/etc…

Version Control

Version	Date	Author	Change Summary
1.1	21/07/2022	L Busher	Formatting changes and review

Contents

1. POLICY INTRODUCTION

This policy is to ensure the Alliance complies with 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 patient records. Cyber security is also addressed during the induction policy for new members of staff.

2. 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. The Alliance will guard against weaknesses in system configurations and promote staff working practices that guard against cyber-attacks.

3. 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.

The Alliance 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 manager must authorise any installation of software.
- The IT manager 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.
- Awareness of malicious ‘hoax’ attacks and procedure for handling them, including reporting to IT Manager.

Staff members being made aware of the above controls, and the responsibilities arising from them, is of primary importance to the Alliance. Staff 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.

4. DEALING WITH CYBER ATTACKS

In the event of a cyber-attack, the Alliance 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.

5. 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 the same as ones used for Alliance-based accounts. Where it is suspected that a password has been compromised, it should be changed immediately.

6. 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 Alliance's Information Governance Lead, who will escalate as appropriate.

7. RESOURCES

Computer and Data Security Procedure [*]

Information Governance - Statement of Compliance Version 12 [*]

Common Cyber Attacks: Reducing the Impact

Cyber Essentials Scheme: Overview

Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks.