Sutton Medical Consulting Centre

Ashfurlong Medical Centre
233 Tamworth Road, Sutton Coldfield
West Midlands B75 6DX
Telephone: 0121 308 7774 Fax: 0121 308 2100
www.suttonmedicalconsulting.co.uk

Information Security Policy

<u>This is a controlled document and must not be copied or distributed without authorisation.</u>

Complied by Consulting Centre Director 1st August 2017

Sutton Medical Consulting Centre

Ashfurlong Medical Centre
233 Tamworth Road, Sutton Coldfield
West Midlands B75 6DX
Telephone: 0121 308 7774 Fax: 0121 308 2100
www.suttonmedicalconsulting.co.uk

Information Security Policy

1.0 INTRODUCTION

- Information is vital to the way that SMCC conducts its business. As the controller of a large volume of valuable information, much of which is highly sensitive, SMCC has a legal, ethical and corporate responsibility to protect that information from unauthorised modification, loss or disclosure, whether accidental or deliberate. In addition, reliable information must be available when and where it is needed for SMCC to undertake day to day business processes.

2.0 OBJECTIVES

The objectives of this Information Security Policy are too:

- Ensure the continuity of SMCC and its services to its staff, customers and business partners.
- Minimise the likelihood of a threat to information security causing loss or damage to SMCC its staff, customers or business partners.
- Minimise the extent of loss or damage arising from a security breach or exposure.
- Ensure that adequate resources are applied to implement an effective information security management programme that delivers the level of security assurance required.
- Inform all SMCC personnel, customers and business partners who have access to SMCC information of their responsibilities and obligations with respect to security.
- Ensure that the principles of information security are consistently and effectively applied during the planning and development of SMCC business activities.

3.0 POLICY

- The purpose of this policy is to provide clear direction and objectives for the management of information security within SMCC in order to protect the organisations information assets from all threats, whether internal or external, deliberate or accidental.
- This Policy is aligned with the best practice standards and information security management.

Continued

Sutton Medical Consulting Centre

Ashfurlong Medical Centre
233 Tamworth Road, Sutton Coldfield
West Midlands B75 6DX
Telephone: 0121 308 7774 Fax: 0121 308 2100
www.suttonmedicalconsulting.co.uk

It is the Policy of SMCC to ensure that:

- Information is protected from any adverse impact that could arise from security failures
- Information is protected against unauthorised access and disclosure
- Confidentiality, integrity and Availability of information will be assured
- Regulatory and legislative requirements are met
- Business Continuity plans produced, maintained and tested
- All breaches of information and physical security actual or suspected, will be monitored, reported and investigated
- Information Security education is available to all staff

SMCC takes a proactive approach to information security risk management, security risk treatment and the prevention of security incidents. In Implementing security in all systems, processes and procedures. SMCC will adhere to the following principles:

- Security will be an integral part of our culture and working practices and security measures will be designed into all projects and processes
- In selecting security controls key criteria will be effectiveness, usability and manageability. All Security Controls will be developed in response to security risk assessment

Security will meet the following objections in order of priority:

- Prevention of incidents – by identifying and reducing risk
- Detection of incidents – before damage can be done
- Recovery from incidents – repairing damage and implementing controls to prevent reoccurrence
- Compliance with security controls will be monitored and audited and all security initiatives will support a process of continual improvement.

4.0 POLICY GOVERNANCE AND REVIEW

- Approval – this information Security Policy is formally ratified and endorsed by the SMCC Directors and supersedes all previous Information Security Policy statements.
- Ownership – This policy is owned and controlled by the SMCC Directors and will be reviewed by them if there is a significant change to business operations, organisation structure, or legal regulatory obligations.

CONTINUED

Ashfurlong Medical Centre
233 Tamworth Road, Sutton Coldfield
West Midlands B75 6DX
Telephone: 0121 308 7774 Fax: 0121 308 2100
www.suttonmedicalconsulting.co.uk

- Classification - This policy is classified as Public and is therefore suitable for internal and external distribution.
- Document Retention and Location – The master copy of this document, and subsequent versions of it, will be retained by the policy owner and within SMCC's Policy storage area.
- Exceptions – Requests for exceptions to this policy must be submitted in writing including business justification to the Directors. Each exemption request will be considered on its merits and granted only on the basis of acceptable levels of risk. Exceptions must be formally approved, endorsed by the Directors and records maintained.

5.0 SCOPE AND APPLICABILITY

- This policy applies to all information assets held by SMCC in any form and will apply to all SMCC business operations that fall under its control.

All personnel working within SMCC must comply with this policy. This includes:

- All permanent Employees
- All Temporary and sub-contracted employees
- All partners, consultant's suppliers, their employees or agents who directly or indirectly support SMCC.

6.0 SECURITY MANAGEMENT

- SMCC Managing Directors and the Consulting Centre Director have overall responsibility for information Governance and Security throughout the Organisation.
- Line managers are responsible for implementing this information Security Policy within the processes and working practices of their responsible areas, and ensuring their staff adhere to the standards and training provided when necessary.
- All Employees are responsible for their own compliance with this policy. It is the employee's responsibility to ensure they make their line manager aware of any training requirements and all employees are required to acknowledge and verify their understanding of this document and the policies relating to information security. Appendix 1

7.0 SECURITY RISK MANAGEMENT

Ashfurlong Medical Centre
233 Tamworth Road, Sutton Coldfield
West Midlands B75 6DX
Telephone: 0121 308 7774 Fax: 0121 308 2100
www.suttonmedicalconsulting.co.uk

- In the event of any information security breech a risk assessment will be carried out by the Consulting Centre Director and the Management team. The assessment will be assessed and reported on and the outcomes relayed to those affected. Analysis of incidents must also include identification of trends and lessons learned to prevent reoccurrence. Incidents must be reported immediately to a line manager.

8.0 HUMAN RESOURCES SECURITY

- SMCC is obliged under legislation, including the UK Data Protection Act 2018, and contractual commitments to ensure that all employees having access to personal data are subject to the appropriate screening during the recruitment process. Background checks on all candidates for employment, must be carried out in accordance with the relevant laws.

9.0 COMMUNICATIONS AND OPERATIONS MANAGEMENT

- In order to do business, SMCC exchanges information internally and externally. All employees are required to consider the sensitivity of the information they are exchanging and ensure they have the appropriate authority to disclose the information, either into the public domain or directly to business partners and third party suppliers. In all cases the amount of information exchanged must be limited to that data that is deemed necessary to fulfil the request. Any data exchange should be conducted in a secure manner.
- All SMCC employees are granted access to email and the internet, however employees are reminded that their use of the systems can be subject to monitoring and that restrictions apply to the exchange of patient identifiable data. Where possible any email exchange where patient data is identifiable should be accessed via the NHS.net account.
- IT access and control is limited to SMCC administrator and employees only. Access to systems will be granted to authorised users only. All employees will be issued with User logins and Passwords. The use of a colleague's security details is prohibited.

10.0 BUSINESS SECURITY AND DISASTER RECOVERY

Ashfurlong Medical Centre
233 Tamworth Road, Sutton Coldfield
West Midlands B75 6DX
Telephone: 0121 308 7774 Fax: 0121 308 2100
www.suttonmedicalconsulting.co.uk

- SMCC Will implement controls to minimise the likelihood of disruption to services caused by disasters or security failure, limit the consequences in the event of such failure and affect a timely recovery. Executive Directors are responsible for creating, managing and testing business continuity plans for the centre.
- To ensure the availability and integrity of information during periods affected by loss of power or network connectivity, and to reduce the impact of machine breakdown, arrangements will include regular and restorable backups are made of data.

11.0 MONITORING AND COMPLIANCE

- Information Security and the monitoring of, is the responsibility of the Executive Directors and Centre Director. SMCC is ICO certified, Register of data controllers, registration reference Z9757906. SMCC will adhere to the legal and regulatory requirements for records retention.
- SMCC will comply with all appropriate legal, regulatory, ethical and contractual requirements for information security including, but not limited to, the following legislation;
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Health and Safety at Work Act 1974
- NHS Contractual Information Governance Obligations
- Human Rights Act 1998
- Public interest Disclosure Act 1998
- Audit Commission Act 1998
- Health and Social Care Act 2001
- Regulation of investigatory Powers Act 2000
- The Caldicott Guidelines
- Common Law

12 VIOLATIONS

Sutton Medical Consulting Centre

Ashfurlong Medical Centre
233 Tamworth Road, Sutton Coldfield
West Midlands B75 6DX
Telephone: 0121 308 7774 Fax: 0121 308 2100
www.suttonmedicalconsulting.co.uk

- Any breaches of this Information Security Policy will be subject to a formal security investigation. Failure to comply with this Policy can result in disciplinary action being taken against individuals under the SMCC disciplinary process, including termination of employment, legal action and referral to law enforcement authorities if warranted.

SMCC appendix 1

Sutton Medical Consulting Centre

Ashfurlong Medical Centre
233 Tamworth Road, Sutton Coldfield
West Midlands B75 6DX
Telephone: 0121 308 7774 Fax: 0121 308 2100
www.suttonmedicalconsulting.co.uk

Policy Sign-off form

Declaration

I have seen and read a copy of the relevant SMCC Information Security Policy Documents. I understand the terms of the relevant policy and agree to abide by them. I understand that security software may record the use I make of the Internet, which may include logging the address of wen sites and noting file transfers make. I understand that any violation of policy may result in disciplinary action, and possibly dismissal or criminal prosecution.

Full Name ……

Signature ……

Designation ……

Date ……

Please sign and return this form to be placed in either your HR or Practising Privileges file.