Somerset Partnership NHS
NHS Foundation Trust

SECURITY MANAGEMENT STRATEGY

2016 – 2019

Security management supports high quality healthcare by providing safe and secure environments which protect patients, staff and visitors and their property and the physical assets of the Trust.

Security management is everyone's responsibility.

Security presents very real challenges in a culture where staff have been trained to always put the patient first. Sensible and cost effective security management initiatives can be taken to reduce risks to patients, staff and visitors

Security involves all groups and levels of staff. To be effective, it is important to establish at the outset the support of everyone in the organisation.

The Board of Somerset Partnership NHS Foundation Trust is committed to ensuring systems and processes are in place, and subject to continuous review, in order to ensure effective management of security risks.

1. INTRODUCTION

1.1 This strategy defines the Trust's approach to security management and its compliance with NHS Protect's Security Management Standards. This document outlines the Trust strategy for tackling crime and reflects the national strategy published by NHS Protect.

1.2 Security management supports the Trust to provide high quality healthcare in safe and secure environments which protects patients, staff and visitors, their property and the physical assets of the organisation. Security management must be managed effectively, efficiently and proportionately.

1.3 The Trust is a large community, mental health and learning disability trust in South West England employing more than 4,000 staff, serving a population of more than 500,000, providing services across an area totalling 1,332 square miles in addition to services in the wider south west region, Dorset and the Isle of Wight.

1.4 The Trust provides a number of locally commissioned in-patient and community services, as well as regional and nationally commissioned specialist services. Some buildings are owned and directly managed by the Trust; others are owned by third party organisations in which staff are expected to follow Trust policy in addition to those of their host. The Trust operates across five local authority areas, with two local acute trusts and two command areas of Avon and Somerset Constabulary.

1.5 The strategy is wide-ranging and considers threats to all Trust processes and will enable security management to be aligned to Trust corporate objectives, values, and priorities.

1.6 The Care Quality Commission (CQC) has identified security and safety as critical parts of good healthcare provision and are included in their standards for NHS providers. As a minimum the Trust must comply with legislation and work with NHS Protect to raise the standards of the service.

1.7 This strategy underpins the Security Policy which is available electronically at http://www.sompar.nhs.uk/media/2905/security-policy-v4mar-2016.pdf.

2. BACKGROUND

2.1 Employees and the public expect to see security mechanisms in their healthcare services. Security management evolved from crime prevention to one of multi-disciplined protective security working proactively alongside a range of agencies. Security management sets out to:

- protect people, property and assets;

- plan and co-ordinate activities to protect the healthcare environment;
- deter, disrupt and prevent deliberate and accidental breaches of security.

2.2 Security management has many elements and should underpin all services delivered by the Trust and will reduce the likelihood of security-related incidents occurring. But security management should not impede the public right of access or have a negative effect on privacy, dignity or quality of care, but nevertheless is vital for the safe delivery of services.

2.3 Security risks may affect:

- patients, staff and visitors;
- buildings and grounds;
- equipment;
- governance and management processes;
- services provided to patients and local communities.

2.4 Security Management aims to reduce the potential for:

- loss of life;
- harm to staff, patients, visitors and the public;
- loss and damage to buildings, equipment and critical assets;
- damage to organisation reputation.

3. SCOPE

3.1 This Strategy includes the following Trust activities:

- clinical;
- financial;
- non-clinical;
- health and safety;
- environmental;
- public and corporate liability.

3.2 The Strategy applies to:

- patients;
- carers;
- staff employed by the Trust (full-time and part-time employees);

- visitors;
- contractors;
- all Trust owned and leased premises and property;
- sub-contractors;
- volunteers;
- all other persons engaged in business on behalf of the Trust.

4. DUTIES

4.1 The **Chief Executive** has overall accountability and responsibility for the implementation of this strategy.

4.2 The **Director of Governance and Corporate Development** has delegated overall responsibility and is the Security Management Director (SMD) for ensuring all security risk and assurance processes are designed, implemented and embedded throughout the organisation. The Director will report any significant issues arising from the implementation of this strategy including evidence of non-compliance or lack of effectiveness so that remedial action can be taken.

4.3 The **Executive Directors,** as members of the Trust Board, have a corporate responsibility to ensure the Strategy is fit for purpose, is implemented effectively and controls are in place to ensure all reasonable care has been taken to manage security proactively. This includes setting clear objectives for line managers to implement the Strategy, to monitor performance against objectives and to act appropriately on this information.

4.4 The nominated **Non-Executive Director** has a corporate responsibility to ensure the Security Management Strategy is to promote security management work at Board level and to challenge, scrutinise and ensure accountability.

4.5 The **Head of Corporate Business** oversees the operational management and delivery of the Trust's Security Strategy; provides advice and guidance on security management issues to the SMD, operational services and to the Health, Safety and Security Management Group. In addition, the Head will provides advice and guidance through submission of reports and attendance at Trust and external agency meetings on statutory, mandatory and Department of Health requirements.

4.6 The **Local Security Management Specialist (LSMS)** works on behalf of the Trust to deliver an environment which is safe and secure so that the highest standards of clinical care can be made available to

patients. The LSMS undertakes duties to tackle violence and general security management; in accordance with training, security standards, advice and guidance provided by the NHS Protect. This is achieved by working in close partnership with stakeholders within the NHS, NHS Protect and external organisations such as the Police, Crown Prosecution Services, other professional bodies and trade unions. The LSMS will work towards the creation of a pro-security culture within the Trust. The LSMS monitors violence and security incident trends and investigate incidents through the Security Incident Reporting System (SIRS) and other sources, to ensure the Trust is taking appropriate action with respect to such incidents.

4.7 **All Staff** are responsible to be familiar and comply with the Trust's security management procedures and processes, to identify, assess, report and to mitigate risks over which they have control in their daily work and to cooperate with their line managers. They are also responsible for undertaking training identified by their line manager and to report known breaches of compliance with security management policies whether by others or by themselves.

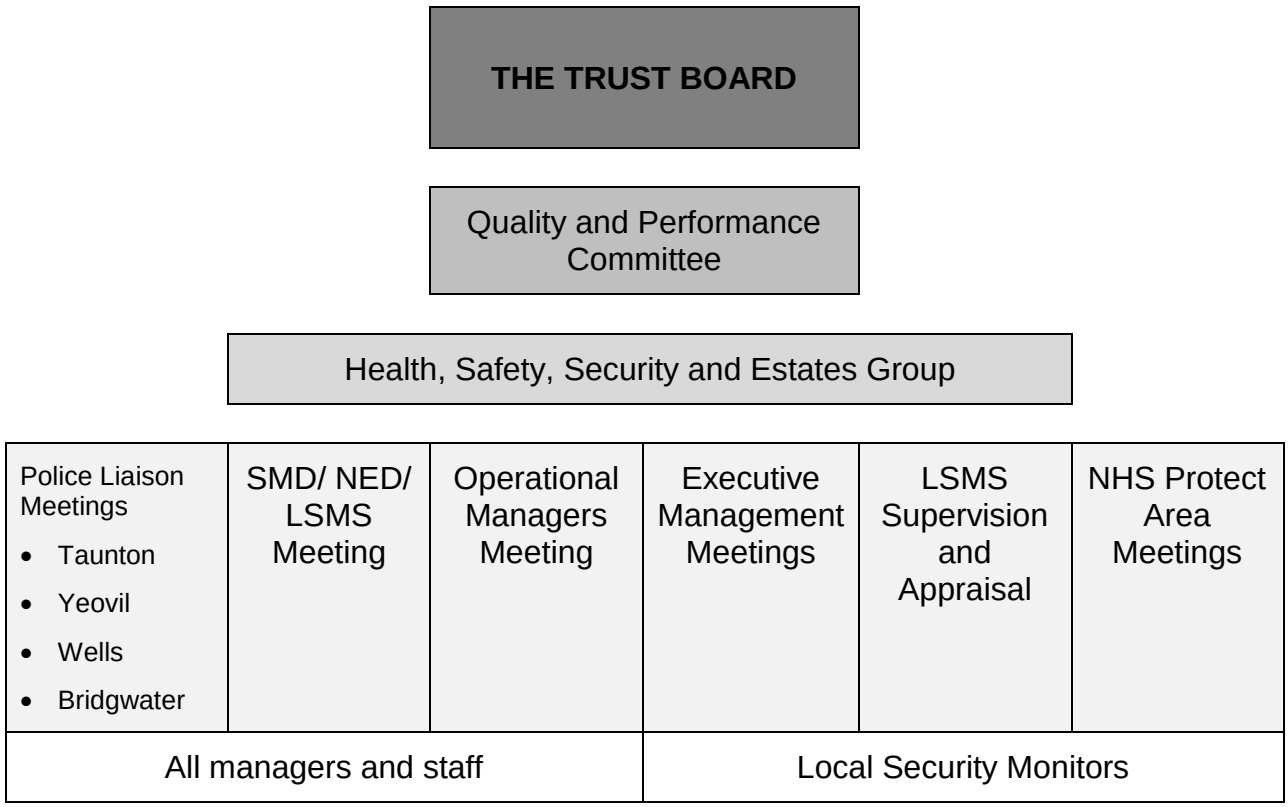
5. GOVERNANCE ARRANGEMENTS

5.1 The broad security management policy framework is illustrated below:

SECURITY MANAGEMENT STRATEGY

Physical Security			Incident Response		Staff Protection		Personnel Security	
Security Policy	CCTV Policy	Patient Property Policy	Lockdown Policy	Incident Response Policy	Lone Working Policy	PMVA Policy	Staff Appraisal and Management Supervision Policy	DBS Policy
							Leavers Policy	ID Badges

5.2 The Trust recognises security management cannot be simply attributed to one person, but is an integral part of its normal management processes. The Trust ensures there is a governance structure is in place to deliver security management through the Trust Board, committees and groups with responsibility for security management:



6. KEY PRINCIPLES

6.1 Creating a **pro-security culture** amongst staff, professionals and the public ensures responsibility for security is accepted by all and the actions of the minority who breach securities are not tolerated:

- **Deterring** those who may be minded to breach security – using publicity to raise awareness of what the consequences of their intended actions could be, both personally and to the NHS;
- **Preventing** security incidents or breaches from occurring, wherever possible, or minimising the risk of them occurring by conducting risk assessments, learning from operational experience about previous incidents, using technology wisely and sharing best practice;
- **Detecting** security incidents or breaches and ensuring these are reported in a simple, consistent manner across the NHS so that trends and risks can be analysed, allowing this data to properly inform the development of preventative measures or the revision of policies and procedures, both nationally and locally;
- **Investigating** security incidents or breaches in a fair, objective and professional manner, to ensure the causes of such incidents

or breaches are fully examined and fed into prevention work to minimise the risk of them occurring again and those responsible for such incidents are held to account for their actions.

6.2 Seeking **redress** through the criminal and civil justice systems against those whose actions lead to loss of NHS resources, through security breaches or incidents, and ensuring that those who are the victims of violence within the NHS environment are supported to seek appropriate compensation from offenders for loss of earning or for the effects of injuries sustained.

7. CURRENT POSITION

7.1 Since the publication of the Trust's first Security Management Strategy in 2013, significant organisational restructuring was realised following the completion of the Integration Phase 2 project resulting in significant changes to way Trust services are organised and managed.

7.2 The Trust acquired dental services in Dorset and the Isle of Wight, which brought fresh security challenges and the need to work with two additional police forces in Hampshire and Dorset.

7.3 The Trust had an inspection visit from CQC in September 2015 during which security management was assessed as part of the assurance process. The organisation will also experience its first NHS Protect inspection visit in August 2016 and will be assessed against the NHS Protect Security Management Standards.

7.4 The backdrop to these was the continued budgetary pressures on the Trust and the need to formulate continued cost improvement plans, one of which was the reduction of Trust LSMS cover available from 1.6 to 1.0 wte.

7.5 These financially challenging times has meant the Trust has necessarily had to concentrate on the direct services it provides to patients and their families, sometimes resulting in projects not being able to be realised.

7.6 A SWOT Analysis of the current position is given below.

SWOT ANALYSIS	
Strengths • new Security and Lockdown policies and associated procedures in place • SMD and LSMS in post • additional senior management for security available; • security action plan and quarterly security reports • good levels of incident reporting from mental health services; • the Trust is in the top 10 NHS Trusts for applying sanctions; • local security monitors in place across services; • the Trust recognises the importance of security management and staff appreciate its interventions	**Weaknesses** • different security cultures between community and mental health services • patchy or no mobile network coverage in parts of Somerset • assets under £5K value not marked • LSMS has limited opportunity to carry out preventative work due to ongoing caseload work • CCTV coverage patchy, poor quality and non-existent in some services • lack of general awareness of security issues and solutions across the Trust • decentralised 'security' budget • reduced incident reporting from community health services • regular loss of ID badges and mobile phones
Opportunities: • develop a new Security Strategy to give further direction and demonstrate assurance • devolve general security management responsibilities to local managers by using the LSMS as a specialist resource • develop stronger, more consistent relationships with partner agencies, particular with operational police officers • develop more robust lockdown plans • develop effective local lone working procedures including improved tracking	**Threats** • change of role for NHS Protect • financially challenging economic climate • healthcare provided in a variety of environments, not all under Trust control and with variable security arrangements • wide geographical area of the Trust • possible hardening position by police services towards mental health and prosecution of cases

8. THE THREE STRANDS FOR ACTION

8.1 There are three key principles which will help to reduce crime and deal effectively with those who perpetrate it against the Trust, its staff, patients and members of the public.

8.1 **Inform and Involve** staff, patients and others who use its services about crime and how to tackle it. They should be informed and involved to increase understanding of the impact of crime through communications and promotion such as public awareness campaigns. Working relationships with stakeholders will be strengthened and maintained through active engagement. Where necessary, the Trust will work to change the culture and perceptions of crime so it is not tolerated at any level.

8.2 **Prevent and Deter** crime to take away the opportunity for crime to occur or reoccur and discourage those tempted to commit crime. Successes will be publicised so the consequences of detection are clear to potential offenders. Those who are not deterred will be prevented from committing crime by robust systems which will be put in place in line with standards developed by NHS Protect.

8.3 **Hold to account** those who have committed crime. Crimes must be detected and investigated, suspects prosecuted where appropriate, and redress sought where possible. This work will be carried out in the main by the police and other crime prevention agencies but with appropriate support from the LSMS and Trust managers. Where recovery of monies lost to crime is viable, this will be pursued. In relation to crimes against staff, criminal damage or theft against NHS property, investigation and prosecution should be undertaken in liaison with the police and Crown Prosecution Service or where necessary NHS Protect.

9 STRATEGIC AIMS

9.1 Security will be improved and crime reduced by targeting work effectively and building in anti-crime measures in all Trust processes and procedures and reflecting the wider NHS initiatives where appropriate.

9.2 The Board, Security Management Director and senior managers will ensure the full implementation of this strategy across the whole organisation. The Head of Corporate Business and the LSMS will take the lead in promoting the strategy and will ensure proactive transition to a more effective security culture.

NHS Protect Standards

9.3 The primary aim of this strategy must be to ensure the Trust's compliance with the NHS Protect Security Management Standards. To

achieve this the Trust will undertake ongoing work planning and an annual review of its security work using the NHS Protect Self Review Toolkit. The results of these will inform the effectiveness of these activities and future, proactive work.

9.4 If crime is to be reduced and security improved, a multi-faceted approach is needed which is both proactive and reactive.

Pro Security Culture

9.5 The development of a pro-security culture is integral to security management and is one where the responsibility for security is accepted by all and whose actions minimise the risks from injury, loss of assets, information and reputation. This leads to improved detection, diversion and investigation of security incidents leading to reduced dishonesty, vandalism, damage and the potential litigation and improves identification of trends and highlight security weaknesses.

9.6 It is the staff who will realise this vision and they need to be prepared for potential changes to some of their practices and perhaps most importantly in terms of lone working safety. Staff want to feel safe and secure at work. Nevertheless, they need to be empowered and motivated to take ownership of security and the initiatives arising from this strategy.

Security Management Work Plan

9.7 The Head of Corporate Business, in association with the SMD and LSMS, will develop an annual work plan informed by the Self-Assessment Tool to take the vision forward. This will set out the key objectives within reasonable and achievable time-scales and a clear statement of the outcomes to be delivered and benefits to be realised from these. A range of targets and performance indicators will be required to ensure effective control of resources and activities.

Communication

9.8 Security management will be communicated by a variety of means and must be a two-way process between the Trust and its staff. The Local Security Monitors in all Trust service areas are integral to this. Methods of communication will include articles in “What’sOn”, newsletters, corporate induction, presentations, leaflets, emails, and posters.

9.9 It is equally important patients and visitors are fully aware of the standards of conduct expected of them and the sanctions which may follow if they behave unacceptably. Collective responsibility, working in partnership with other agencies, is essential so that local ownership for security is shared. Where the responsibility for security is accepted by all and a strong message communicated to the staff, patients and

members of the public alike that violence, whether physical or verbal, will not be tolerated incidents can be reduced.

9.10 The Trust's primary focus must be prevention rather than punitive redress in the main regarding workplace violence. The Trust must actively build in robust accountability regarding the protection of its assets and will take legal redress to recover losses from theft or acts of criminality.

Working in Partnership

9.11 The Trust will need to work in close partnership with the local police in accordance with the Crime and Disorder Act, the local authorities and community safety forums. Intelligence exchanged between the Trust and these organisations will help inform the Trust of particular areas of concern for which crime prevention strategies can be implemented locally.

9.12 The strategy will enable security management to support high quality healthcare by providing safe and secure environments which protect patients, staff and visitors and the physical assets of the Trust.

9.13 But security management must be everyone's responsibility.

9.14 Security management presents real challenges to healthcare where staff are trained to put patients first. But sensible and cost effective initiatives will be taken to reduce risks to patients, staff, carers and others environments which prevent criminal activity.

ANDREW SINCLAIR

HEAD OF CORPORATE BUSINESS