

# Security Strategy



## Document Summary

This document sets out Cumbria Partnership NHS Foundation Trust's strategy for security management, and in particular how it will adopt and implement NHS Protect Security Management protocols and standards.

<b>DOCUMENT NUMBER</b>	<b>POL/002/015/001</b>
<b>DATE RATIFIED</b>	October 2015
<b>DATE IMPLEMENTED</b>	October 2015
<b>NEXT REVIEW DATE</b>	October 2018
<b>ACCOUNTABLE DIRECTOR</b>	Director of Strategy and Support Services
<b>POLICY AUTHOR</b>	Head of Corporate Governance

## Important Note:

**The Intranet version of this document is the only version that is maintained.**

Any printed copies should therefore be viewed as "uncontrolled" and, as such, may not necessarily contain the latest updates and amendments.

## TABLE OF CONTENTS

1	SCOPE.....	3
2	INTRODUCTION.....	3
3	AIMS AND OBJECTIVES .....	3
4	DEFINITIONS .....	3
5	ROLES AND RESPONSIBILITIES.....	4
6	ARRANGEMENTS.....	4
7	TRAINING.....	6
8	MONITORING COMPLIANCE WITH THIS DOCUMENT .....	6
9	REFERENCES/ BIBLIOGRAPHY .....	7
10	RELATED TRUST POLICY/PROCEDURES .....	7
	EQUALITY IMPACT ASSESSMENT.....	<b>Error! Bookmark not defined.</b>
	DOCUMENT CONTROL CHECKLIST .....	<b>Error! Bookmark not defined.</b>
	The Golden Rules .....	<b>Error! Bookmark not defined.</b>

## 1 SCOPE

1.1 This strategy applies to all services and at all levels throughout the Trust.

## 2 INTRODUCTION

2.1 This document sets out Cumbria Partnership NHS Foundation Trust's strategy for security management, and in particular how it will adopt and implement NHS Protect Security Management protocols and standards.

## 3 AIMS AND OBJECTIVES

3.1 The Trust aims to ensure it has safe and secure environments which protect patients, clients, visitors, staff, professionals and contractors, their property and the physical assets of the organization. This will be delivered through the implementation of arrangements described within Trust policies and procedures including, but not limited to, the following:-

- Risk and Safety Strategy and Policy
- Security Policy
- Lone Working Policy
- Preparing for a Serious Security Occurrence (Lockdown) Policy
- Health and Safety Policy
- Service Delivery Health & Safety Risk Assessment Policy.
- Information Governance Strategic Management Framework
- Medical Devices Policy
- Information Security policy

3.2 The Trust will:-

- allocate resources to identify and manage security management risks,
- implement NHS Protect standards and protocols for security management
- inform and involve key stakeholders,
- prevent and deter security incidents,
- hold to account those with responsibilities for security management
- continually review security management performance
- report on security management performance
- adopt a risk-based approach to security management

## 4 DEFINITIONS

4.1 Definitions for security management are outlined within the Security Policy (POL/002/015)

## 5 ROLES AND RESPONSIBILITIES

- 5.1 The Trust will employ staff in the roles of Security Management Director (SMD), and accredited Local Security Management Specialist (LSMS).
- 5.2 Roles and responsibilities for security management are set out within the Trust's Security Management policy.

## 6 ARRANGEMENTS

- 6.1 The Trust will employ at least two LSMSs, one of which will be designated as 'Lead LSMS'. At least one LSMS will attend NHS Protect regional network meetings on a quarterly basis.
- 6.2 Arrangements for reporting and investigating security related incidents, and support to staff in the event of a security incident, will be managed in accordance with the Trust's Incident and Serious Untoward Incident and Near Miss Reporting Policy and Untoward Incidents/Formal Complaints/Claims/ Investigation Policy (POL/002/006 and POL/002/006/001).
- 6.3 Identification and management of security management risks will be undertaken in accordance with the Trust's Risk and Safety Strategy and Policy (POL/002/012) and the Service Delivery Health and Safety Risk Assessment Policy (POL/002/023).
- 6.4 Arrangements for the management of lone working will be managed in accordance with the Trust's Lone Working Policy (POL/002/057).
- 6.5 Arrangements for the management of Lockdown are described within the Preparing for a Serious Security Occurrence (Lockdown) Policy (POL/002/070).
- 6.6 Arrangements for the identification, management, purchase and disposal of Trust assets will be managed in accordance with Trust financial procedures, and also in accordance with relevant policies. Asset registers for medical devices will be managed and coordinated by the Medical Devices Officer in accordance with the Infection Prevention and Control: Medical Equipment Policy (POL/001/042/023). Asset registers for IT-related equipment will be managed by the IT Department in accordance with the Trust's suite of Information Governance policies. Responsibility for management of assets at a departmental / service level is delegated to service managers. This is set out within the Trust's security management policy. LSMSs will have no

---

direct involvement or responsibility for the management or maintenance of asset registers.

6.7 The Trust will complete and submit the NHS Protect self-assessment against NHS Security Management Standards.

6.8 The Lead LSMS will ensure an annual work plan for security management is developed, regularly reviewed, and reported upon.

6.9 LSMSs have no direct responsibility for the management of the Trust's incident reporting system. They will, however, work with the Safety Quality and Safeguarding Team who lead on incident reporting system, to ensure submission of reports to NHS Protect, including annual reports on security management performance, and notification of security incidents to the Security Incident Reporting System (SIRS)

6.10 The Trust will implement the NHS Protect PREVENT strategy. This will be led by the Trust's Nursing and Quality Directorate Safeguarding team, and supported by LSMS.

6.11 Performance on security management will be reported as a minimum to:-

- the Corporate Fire, Health, Safety & Security Committee as a standing item on its agenda.
- the Trust Management Group, on a frequency that is in accordance with that Committee's annual work plan.
- Care Group and Service managers via feedback on reported incidents coordinated by the Safety Quality & Safeguarding team

6.12 Conflict Resolution Training (CRT) will be delivered as part of the Trust's training programmes for the Prevention and Management of Violence and Aggression (PMVA) and Risky Business, both of which form part of the Trust's mandatory training programmes. Arrangements for the management of Trust training programmes are set out in the Trust's Learning and Development policy (POL/004/037) and Training Needs Analysis (TNA). The Trust's Organisational Learning and Development department are responsible for the delivery of the Trust's training programme and for ensuring that training minimum requirements in relation to content, delivery mechanisms and frequency of delivery. LSMSs will work with Organisational Learning and Development to ensure they have all relevant information about CRT requirements in order that appropriate training programmes can be delivered.

6.13 The Trust does not directly employ staff in dedicated 'security' roles, for example security guards or security officers, at any of its work bases. This

---

arrangement will be periodically reviewed, taking into account reported security incidents following a risk-based approach to security management, on a site-by-site basis.

6.14 The Trust will on a periodic basis, consider whether to invoke the discretionary powers under the CIJA Act (state in full) in relation to the managing disturbance behaviour on Trust premises. This decision will be taken by the Trust Management Group. The Trust's current position is that it will not invoke those discretionary powers.

6.15 The Trust will adopt Memorandum of Understanding (MOU) agreed by the Area Security Management Specialist (ASMS), and will build and maintain relationships with the local regional police service in order that there are clear points of contact for LSMSs and service managers.

## 7 TRAINING

7.1 There are no training implications associated with this Strategy

## 8 MONITORING COMPLIANCE WITH THIS DOCUMENT

The table below outlines the Trusts' monitoring arrangements for this policy/document. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

Aspect of compliance or effectiveness being monitored	Monitoring method	Individual responsible for the monitoring	Frequency of the monitoring activity	Group / committee which will receive the findings / monitoring report	Group / committee / individual responsible for ensuring that the actions are completed
Performance against annual work plan	Annual work plan and report	Safety and Security Officer	Annual	Corporate Fire, Health, Safety and Security Committee.  NHS Protect	Head of Corporate Governance
Performance against NHS Protect security standards	NHS Protect self-assessment submission against security standards	Safety and Security Officer	Annual	Corporate Fire, Health, Safety and Security Committee.  NHS Protect	Head of Corporate Governance

## **9 REFERENCES/ BIBLIOGRAPHY**

9.1 NHS Protect Security Management Standards

9.2 NHS Prevent strategy

## **10 RELATED TRUST POLICY/PROCEDURES**

- Trust's Risk and Safety Strategy and Policy (POL/002/012)
- Security Policy (POL/002/015)
- Lone Working Policy (POL/002/057)
- Preparing for a Serious Security Occurrence (Lockdown) Policy (POL/002/070).
- Health and Safety Policy (POL/002/019)
- Service Delivery Health & Safety Risk Assessment Policy (POL/002/023).
- Information Governance Strategic Management Framework
- Infection Prevention and Control: Medical Equipment Policy (POL/001/042/023)
- Information Security policy
- Incident and Serious Untoward Incident and Near Miss Reporting Policy (POL/002/006)
- Untoward Incidents/Formal Complaints/Claims/ Investigation Policy (POL/002/006/001).
- Learning and Development Policy (POL/004/037)