NHS Shetland

Security Policy

Date: **April 2015**

Version number: 2

Author: **Head of Estates and Facilities**

Review Date: **April 2018**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

NHS SHETLAND DOCUMENT DEVELOPMENT COVERSHEET*

Name of document	**Security Policy**	
Registration Reference Number	**CE POL 10**	**New** □ **Review** ☒
Author	**Lawson Bisset**	
Executive Lead	**Ralph Roberts**	

Proposed groups to present document to:	
Health and Safety Committee	Staff Governance
APF	
Executive Management Team (EMT)	

DATE	VERSION	GROUP	REASON	OUTCOME
6th May 2015	2	Health and Safety Committee	C/S	Approved
14th May 2015	2	APF	C/S	Approved
27th August 2015	2	Staff Governance	C/S	Approved
14th Oct 2015	2	EMT	C/S	Approved

Examples of reasons for presenting to the group	Examples of outcomes following meeting
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)

DATE	CHANGES MADE TO DOCUMENT
Oct 2015	Prevent Protocol added to policy

Contents- Sections

SHETLAND NHS BOARD

SECURITY POLICY

1. Introduction

Shetland NHS Board places the health, safety and security of its patients, staff and visitors throughout NHS Shetland as one of its top priorities and will endeavour to maintain safe and secure conditions throughout the organisation.

The Security Policy encompasses personal safety to patients and staff alike and the physical environment and protection of NHS property. There are a number of security issues such as NHS Fraud and Information Governance which due to the specialised nature of these areas are subject to their own Policy and are therefore excluded from this Policy. A list of additional policies covering Security related issues is at Section 13.

Most security issues can be attributed to a combination of factors such as; building design (physical environment), lack of management and non compliance with policy and procedures, lack of managerial and individual ownership of responsibility regarding security issues, training deficiencies and criminal intent. It is essential that everyone accepts their personal and collective responsibility for security and ensures their active co-operation at all levels of the organisation in promoting and maintaining a safe and secure working environment.

NHS Shetland will work to implement the strategies and procedures developed to create a safe and secure working environment.

The Policy will be brought to the attention of all employees and any others with a legitimate interest who may require to be aware of its contents. This Policy will be disseminated to all staff as part of the Corporate Induction and Compulsory Refresher.

2. The Aim of the Policy

The aims of the Policy are to ensure the management of security is effective so that the following is achieved:

- The personal safety of patients, staff and visitors.
- Security of NHS Shetland property, buildings and assets.
- Security of patient's and staff's personal property.

3. Accountability throughout the Organisation

The Chief Executive Officer has the overall responsibility for Security within NHS Shetland; authority is delegated for the implementation of the Security Policy to all managers.
The Head of Estates and Facilities is the Nominated Security Manager who is responsible for ensuring effective security procedures and practice is implemented at an operational level throughout the organisation.

General Managers and Practice Managers through their service and line management structure are operationally accountable for security of their Wards, Departments and Premises. Security arrangements must be put in place to prevent, respond to, report and take measures to prevent re-occurrence of failures in security.

Service, Ward and Departmental Managers have day to day accountability for the overall security within their service, ward or department. All necessary measures must be undertaken to ensure; the security of NHS property, the personal property of patients, the personal safety of patients, staff and visitors and the suitable provision for security of staff's personal belongings whilst at work.

All Members of Staff have an individual and collective responsibility for maintaining a secure and safe working environment and are to cooperate with management and comply with any measures put in place or undertaken in the interests of security and safety.

The Security Manager and the Risk Management Department provides general and specialist advice through specialist advisers (NHS Grampian) for the management of security, and violence and aggression. The Health and Safety / Security Manager are responsible for providing advice on policy and strategy, crime prevention and responding to incidents.

4. Operational Accountability

Ward, Building, and Department Managers will be operationally accountable for day to day management for maintaining security in their building, ward or department, based on the security threat and level of risk that the building, ward or department is exposed to.

4.1 Risk Assessment

A security risk assessment is to be undertaken by the building, ward or department manager; to identify any potential threats, people (patients, staff and others) the work activities involved, and existing control measures. Evaluate a risk rating; identify weaknesses and additional security measures to be taken and implement an action plan to mitigate the risk.

Issues to be considered to include, but not exclusively are; security of the physical environment (doors, windows, locks, keys), working times /shift changes, unscheduled visits, face to face meetings with the public or patient, money transfers, the secure storage of drugs and medicines, high valued or attractive equipment, security of NHS property, security of vehicles and equipment in transit, patient's property, personal safety and personal belongings. (Lone working and community visits to be considered but subject to a separate risk assessment).

4.2 Building / Ward / Department Security Procedures

Managers are to ensure there are written building / ward / departmental security procedures for their area of responsibility. Such procedures to include those issues noted from the risk assessment, working hours, safe management and custody of keys, authorised key holders, department opening up and closing down procedures, receipt and delivery of mail, working out of normal core hours, management of patient visitors and any other matters pertaining to the security of the ward or department.

Such procedures should be completed, reviewed and updated on an annual basis and submitted to the Security Manager.

4.3 Members of Staff

All members of staff have an individual responsibility to cooperate with management and comply with any measure or procedure which has been put in place or undertaken in the interests of security and safety. Staff are to comply with duties assigned to them by management to secure property and equipment and the management of patient's safety and belongings. To have a general awareness of security issues/threats within their ward / department work but also generally throughout the hospital/site. Staff are to report any suspicions or weaknesses to line management and report risks/incidents via Datix system

4.4 Staff Training

Staff training meeting the Partnership Information Guidelines (PIN) recommendations (Scot Gov, 2003) and the Good Practice Statement on the Prevention and Management of Violence (CRAG, 1996) will be offered to all staff and in the first instance will be prioritised to all the identified high risk staff following each building / ward / and departments security risk assessments.

This is anticipated to be;

- Health centre managers and a designated deputy
- Accident and Emergency staff
- Reception staff
- Hospital manager / Senior Nurse Bleep holders Reception staff
- Community nurses
- Ward Managers

Staff Development provide suitable training in house and can provide further details about the design and delivery of training.

4.5 Procedure

In the event of a member of any staff becoming aware or involved in a potential or actual security incident they should;

1. Evaluate and Risk assess the potential or actual security incident and take action as appropriate ensuring their own personal safety and that of those in their care.

2a. If required inform the **POLICE** either directly, via reception, or via a request to another member of staff or via a member of the public immediately or as soon as practically possible of any incident or potential incident.

2b. If required, staff should remove themselves and potentially those in their care to a place of safety until the Police can attend the incident or potential incident.

2c. Inform reception directly or via a request to another member of staff or via a member of the public immediately or as soon as is practically possible of any incident or potential incident.

3a. Reception to confirm with Police that they are responding to the incident.

3b. Reception to inform appropriate senior staff member as listed below;

SITES	**PERSON TO CONTACT**
GBH	Senior Nurse on Call (GBH)
Health Centres	Primary Care Manager
Community Nursing	Chief Nurse (Community)
Dental Practises	Business Manager Dental
Staff Accommodation	Security Manager
Mental Health	Mental Health Manager

3c. Reception to inform the Senior Manager on Call.

3d. Reception to inform Security Manager.

4.6 Security Services

4.6.1 This Policy does not advocate the use of NHS Shetland staff as designated Security Staff at any time.

4.6.2 NHS Shetland anticipate that on occasions it may be necessary to employ out sourced security services who must comply to the NHS National Services Scotland Security Services Standards for NHS Scotland (February 2014).

4.7 Prevent Strategy

4.7.1 The Counter-Terrorism and Security Act 2015 places a duty on the NHS, to have, "*due regard to the need to prevent people from being drawn into terrorism*", in Shetland this also applies to the Police, Local Authorities and Further and Higher Education. CONTEST is the UK Government's counter-terrorism strategy of which The *Prevent* Strategy, is one strand. ***Prevent:* to stop people becoming terrorists or supporting violent extremism.**

4.7.2 We as NHS staff have valuable experience in protecting vulnerable people, and this places Health Boards in a key supportive position. All staff need a general awareness of *Prevent* and to feel ready to deal with concerns when they arise. Vigilance and early intervention, together with an understanding within the NHS of the risks and threats, is paramount.

4.7.3 **Mitigation – Local Protocol**
In respect of progress to date, the specific planned local actions to mitigate the risks posed to NHS staff include:

Staff training:

1. Ensuring that all staff have access to training and information and an awareness of Prevent concerns
2. All staff should know how to raise a concern:

- Discuss in the first instance with line manager,
- Line manager's action will depend upon concern raised but will want out **check** out the concern and **share** appropriately.
- Sources of advice are NHS Shetland: wendy.hatrick@nhs.net, janice.irvine@nhs.net

3. Front-line staff will have access to suitable training and should know how to raise a professional concern in relation to a young person:

- Discuss a Prevent related concern with line manager / Child's named person,
- Use Getting It Right For Every Child (GIRFEC) interagency screening meeting or make a child protection referral to the duty social worker
- Following an interagency discussion a plan will be formulated to assist chid or young person and their family

Venues Premises and Publicity

4. Ensuring that NHS owned facilities / buildings are not used for meetings / activities or for issuing propaganda that support radicalisation. In agreeing the use of Board facilities for meetings:

- Staff should understand the nature of the meeting and be alert to possible issues of a radical nature or behaviours likely to raise a concern.

5. Board sanctioned publicity via social media or web pages do not provide a platform for extremists / dissemination of extremist views

Policies and Procedures

6. All Policy and Procedures which relate to Board business relevant to Prevent concerns will be updated to include relevant information and practice, for example Child and Adult Protection procedures.

7. Highlighting use of Board's risk register and adverse events / incidents procedure to report Prevent related risks / incidents.

4.7.4 We are all responsible for ensuring existing arrangements for protecting vulnerable adults and children, and use of NHS buildings and facilities, are adapted as necessary so that *Prevent* is mainstreamed and embedded into frontline healthcare services.

5. Property

5.1 Property

Staff, are to take all reasonable steps to safeguard NHS Shetland property in their care.

Members of staff are not to remove NHS property from the workplace, whether the intent is to return it or not without authority of line management. Failure to seek authority from line management will result in disciplinary action and or criminal proceedings being taken.

Staff must take responsibility and take adequate precautions to ensure the security of their personal property and not to bring valuables to work. Where a locker is provided for personal use, the individual to whom it is allocated will be responsible for security.

All patients and patient's relatives are to be made aware of the procedures for safeguarding moneys and valuables. Receipts must be issued for items handed over for safekeeping. NHS Shetland does not accept liability for the theft or damage of any moneys and valuables not handed in for safekeeping.

For further information on the management of patient's property refer to the Standing Financial Policy Section17.

5.2 Equipment Inventory

Building, Ward and department managers are to compile and to keep up to date an inventory of moveable items of equipment which present an attractive target to the thief. USB memory sticks, external hard drives, laptops, ipads, desktop computers and computer ancillaries, televisions, radios or any other item of equipment which can easily be picked up and concealed.

The list is to include the following details; a description of item, the manufacturer, model, colour, serial number, power rating and any other distinctive detail where available. The list will provide an accurate description of any stolen item to be given to the Police to aide in the recovery of stolen goods and possible prosecution.

The list may comprise of Photographic catalogue.

Take ownership of the equipment you hold and do not rely on others; for instance, IT or Medical Physics for information in regards to your computers/equipment.

5.3 Medical Equipment Inventory

Ward, building and department managers are to compile and to keep up to date an inventory of medical equipment of which the ward or department has use of.   The inventory is to be used as a register to track individual items of equipment, which have gone off the ward/premises for maintenance and repair or loaned to another ward or department.

5.4 Security Marking of NHS Equipment

Where practical all items of equipment are to be marked as the Property of NHS Shetland.

5.5 Lost and Found

Items lost and found within the Gilbert Bain Hospital / NHS premises are to be handed into their Reception who will record a description of the item and the details of circumstances relating to the loss or find.

5.6 Staff Collections (Lists)

The collection of money (lists) for birthdays, weddings, nights out and such is to be discouraged, however managers are to ensure if such collections are being undertaken that there are in place suitable arrangements for accountability and security.

6. Security of Premises

6.1 General

- Entrances; main entrances to each building are to be clearly sign posted and where applicable have internal directional signs indicating wards, departments, clinics and reception areas.
- All entrances are to be kept free from obstructions including cars or delivery vehicles at all times.
- Staff are to be aware of all exits particularly emergency exits.
- All external lighting and security lighting is to be fully operational and any defects must be reported to the Estates Department.
- Emergency evacuation; it is essential that staff are aware of the need to quickly and calmly evacuate from the building in the event of; fire, bomb threat, or other emergency. Staff are to be aware of the designated assembly point for their place of work and must report to the assembly point to ensure all staff is accounted for. Staff are to be aware of the procedure for the evacuation for Visitors to the building in the event of an emergency.

6.2 Physical Security

Maintaining the security integrity of NHS premises is a collective responsibility of management and staff. Building, Ward, and Department Managers are to ensure that there are written local procedures and arrangements in place detailing:

- Inspecting, maintaining and reporting faults of all security measures, such as; main access/room/fire exits doors are closing properly and can be secured,

locks and keys, window glass, fasteners and stays, secure cupboards and cabinets are functional.
- Locking up procedures; closing/locking windows and room doors, check external doors including fire exits, securing equipment, locking cupboards, switch off electrical equipment and lights (other than security lights), personnel accounted for/head count, fire check.
- The use of any Intruder alarms; how to set and to unset, and the departmental response to activation.
- Opening up procedures; look and check all is correct – signs of disturbance.
- Core Working Hours.
- List of names of department staff.
- List of authorised key holders.
- Access/management of keys.
- After hours working arrangements.
- Domestic Services arrangements.
- Control of visitors, maintenance and contracted workers accessing restricted areas.
- Receipt and control of mail and delivery of goods/equipment into the department.
- Other security arrangements pertaining to a particular building, ward or department.
- Access codes for digital locks are to be closely controlled to deter wide dissemination of the number, requests NHS Estates to change the code if the number is thought to be compromised.

Such procedures are to be reviewed and updated as necessary. Staff are to be informed and instructed in the use of such procedures and are required to comply with them.

6.3 Controlled Access and Restricted Areas, and Signage

Some buildings and departments such as; Montfield Offices, Theatres, Laboratories Pharmacy or Estates may operate a controlled access system as part of their security management system. Managers are to ensure that the system is managed, supervised and that there is a written procedure which is effectively communicated to all relevant staff. Controlled access systems can include; visitor's register and pass escorted visits and meetings by appointment only. The procedure is to include a visitor's safety brief including emergency evacuation procedure to be given at the time of the visit.

Buildings, departments, stairways, corridors which have deemed to be restricted with no public access; are to be clearly signed; "Staff Only" or "Authorised Persons Only" or "No Public Access". Signs clearly inform the public of restricted access and greatly assist the Police in the arrest of intruders found within such a restricted areas.

6.4 Decommissioning of NHS Premises

The vacating and decommissioning of NHS premises presents several risks; primarily the need to secure any patient identifying or sensitive records - paper or electronic media.
Scottish Government: Records Management Guidance Note 008 Decommissioning of NHS Premises
The link to this document addresses the concerns and makes recommendations relating to the use of disused buildings and the storage of health records or other person identifiable information. These principles can be extended to include all security in general:

- Disused buildings should not be used for storage of any health records or other person identifiable information.
- All sites should be effectively sanitised prior to being vacated; this to be checked and confirmed by effective sweeping and thorough inspection, and fully documented before the site is handed over to a new owner.

If a building is to be left for a period of time prior to disposal the physical security of the building/s needs to be considered, is there a need to:

- Board up the windows and doors
- Isolate services as such as water supply, gas and electricity.

Additional security measures may be required such as CCTV or intruder alarms.

A risk assessment/s is required to determine the risk and the level of physical protection required to deter; vandalism, theft of metal infrastructure, wilful fire raising and any other identifiable risk.

7. Incident Reporting and Recording

7.1 Incident Types

Security incidents may include the following although the list is not exhaustive:

- Loss or theft of NHS property e.g. equipment, stores.
- Damage and acts of vandalism.
- Wilful fire raising.
- Loss of NHS ID badges, fobs and keys.
- Theft of personal property from NHS premises; patients and staff.
- Any act of violence and aggression in relation to staff, patients or members of the public, including; general disorder, threatening behaviour, verbal abuse, hate crime, racial abuse, sectarian abuse, physical assault.
- Breach of security measures.
- Failure in security procedures; failure to lock premises, secure equipment.
- Intruders and unauthorised or unmanaged visitors within restricted areas.
- Threat or physical assault involving staff.
- Other acts of criminality.

7.2 Incident Reporting

7.2.1 Management

It is essential that all security incidents are reported without delay to Ward/Department and Unit management and the details of the incident is reported through the Incident Reporting System (Datix).

7.2.2 Police

Any incident that there is a suspicion of or actual criminal act/s involved is to be reported to the **POLICE** immediately, **telephone 999.**

Any incident that involves, an immediate or potential threat or danger to a person is to be reported to the POLICE immediately, **telephone 999**.

1. Inform the **POLICE** either directly, via reception, or via a request to another member of staff or member of the public immediately or as soon as practically possible.

2. Inform reception immediately or as soon as is practically possible of any incident or potential incident by dialling 0 internally or 01595 743000 externally.

3a. Reception to confirm with Police that they are responding to the incident.

3b. Reception to inform appropriate senior staff member as listed below:

SITES	**PERSON TO CONTACT**
GBH	Senior Nurse on Call (GBH)
Health Centres	Primary Care Manager
Community Nursing	Chief Nurse (Community)
Dental Practises	Business Manager Dental
Staff Accommodation	Security Manager
Mental Health	Mental Health Manager

3c. Reception to inform the Senior Manager on Call.

3d. Reception to inform Security Manager.

7.2.4 Information Governance

An incident involving the loss or theft of moveable media (i.e. ipads, laptops, mobile telephones) must be reported immediately to Information Governance; **(01595 743210)**.

7.3 Post Incident Investigation

An investigation of all incidents is to be undertaken by Managers and reported-in accordance with the NHS Shetland Incident Management Policy The assistance of the Risk Manager / Security Manager can be sought.

8. Identity

8.1 Staff Badges

8.1.1 ID Badge Issue

All staff are to be issued with a NHS Shetland Identity Badge (ID) and they are required to ensure that it is visible at all times, whilst on duty. NHS ID badges are issued for staff from Human Resources. The issue of an ID badge is made by an application authorised by the Line Manager.

8.1.2 Lost ID Badges

Lost or stolen ID badges are to be reported to the employee's line manager (ward, building or department manager) who will record the circumstances relating to the loss and report the loss through the Incident Reporting System (Datix). Staff are to apply through their ward/department manager to Human Resources to obtain a replacement ID badge.

8.1.3 ID Badge on Leaving Employment

When a member of staff leaves the employment of NHS Shetland, the ID badge must be surrendered to the line manager and returned to Human Resources.

8.2 Challenging Identity

In areas where there is restricted and controlled access, unauthorised or unrecognised visitors are to be approached in a polite and non threatening manner; such as asking the person "are you lost" or "can I help you". Remember a person with criminal intent will present themselves often in a genuine manner and may give a feasible answer for their presence; staff are to explain that the person is in a "staff only" part of the hospital and direct them to a public area.

If a person is wearing a NHS staff badge and yet their behaviour seems odd and out of place or the person is not recognised as a known member of staff, challenge their identity, introduce yourself and ask as above "can I help you".

In public areas; staff are to be aware of persons who are acting suspiciously or who seem to be out of place, observe from a distance note the persons description and enlist the help of other staff members. If you feel in anyway unsafe or unsure and the situation merits it, telephone the Police. Report the incident to your department/ward/building management and subsequently via the Incident Reporting Procedure.

All NHS staff are to be aware of bogus tradesmen/workers/sales representatives and if there is a doubt are to challenge the identity and presence; contact as appropriate **NHS Estates (01595) 743684. Security Manager (01595 74 3029**)

9. Control of Visitors

9.1 Ward Visitors

Management of visitors to In-patients wards is controlled locally by ward management with written procedures to include such as; restricted visiting hours and the number visitors per bed in place and so forth. If there is an incident or a visitor's behaviour is becoming a concern notify **POLICE** immediately, give clear details of the situation, ward location and your name.

1. Inform the **POLICE** either directly, via reception, or via a request to another member of staff or member of the public immediately or as soon as practically possible.

2. Inform reception immediately or as soon as is practically possible of any incident or potential incident

3a Reception to confirm with Police that they are responding to the incident.

3b. Reception to inform appropriate senior staff member as listed below;

SITES	**PERSON TO CONTACT**
GBH	Senior Nurse on Call (GBH)
Health Centres	Primary Care Manager
Community Nursing	Chief Nurse (Community)
Dental Practises	Business Manager Dental
Staff Accommodation	Security Manager

3c. Reception to inform the Senior Manager on Call.

3d. Reception to inform Security Manager.

9.2 Visitors to Patients in Custody

For Patients in Custody who have been admitted to hospital from HM Prisons, the responsibility for the control and supervision of visits to these patients lies with the Scottish Prison Service (SPS) and the SPS contracted escort service - G4S. Application for authorised visits to these patients must apply through the SPS as per SPS Policy.

Patients in Custody attending as an outpatient to NHS Shetland premises are also in the control and supervision of the SPS, G4S or the Central Scotland Police.

NHS staff must not accept under any circumstances, gifts of any description from visitors or others for passing on to patients in custody. NHS staff are to refer all such requests to the escorting officers

9.3 Contractors

Ward and Department Managers are to ensure of the identity and authority of maintenance and contractor workers (Estates and Contracted) be aware of the bogus worker. Check with NHS Shetland Estates telephone 01595 743684

All external maintenance, contracted workers and NHS Estates workers are to report to ward/clinic/department/building management on arrival. Technical control and supervision of work is the responsibility of NHS department employing the contractor. Close liaison between the contractor and ward /clinic / department / building management is to ensure all managers are aware of the scope of work involved, restrictions to the ward/department/clinic/building activity, Infection Control and safety measures to be undertaken.

Contractors must closely manage the security of their tools, equipment (ladders), materials and substances within the confines of their work areas to ensure the safety of patients.

9.4 Locum and Agency Staff

Locum and Agency Staff are to report to the person in charge of the ward, facility, health centre or clinic with their identity

10. Management of Keys

10.1 Management of Keys

Management of keys within a ward, building or department is the responsibility of the line manager. A register is to be maintained with details for each key:

- where the key is for
- the type of key
- the key identity number (if marked)
- number of copies
- named key holder/s.

The line manger is to ensure that individual staff members sign for the key. When a member of staff leaves the employment of NHS Shetland, the key is to be surrendered to the line manager.

10.2 NHS Shetland Area Wide

NHS Shetland Estates manage the issue of access keys and fobs. Additional or replacement keys will be supplied by Estates on application by the ward or department line manager; the application to include the reason for the issue.

Following the issue of keys by Estates; Ward or Department are thereafter responsible for the management of all keys that are held within the department / ward.

10.3 Lost Keys

Lost or stolen keys and fobs are to be reported to the employee's line manager (Ward/Departmental Manager) who will record the circumstances relating to the loss and report it via the Incident Reporting System (Datix).

11. Panic Alarms

The provision of panic and personal attack alarms (installed or mobile) are a control measure that is put in place when required as identified by the ward/building or department risk assessment. Where alarms are provided, managers must ensure that there is a local written procedure in place which will direct staff to respond safely and efficiently to any alarm activation. Managers shall ensure that staff that are expected to provide immediate assistance will receive an appropriate level of training in the Management of Violence and Aggression In the absence of dedicated security staff there are no additional staff to respond to an alarm but it may be used to call the police covertly in a sensitive situation.

The written alarm procedure to include a signing in / out sheet for portable alarm devices; it is of the line manager to manage the system and account for all devices held by the department / ward.

12. Monitoring

In order to demonstrate the effectiveness of the policy, statistical information relating to all reported incidents affecting the organisation, staff, patients or members of the public will be collated through the Incident Reporting System (Datix).

The measurement of security performance will comprise proactive and reactive monitoring systems. Managers are to carry out annual reviews of their security risk assessments to proactively ensure the implementation of standards and the effectiveness of management controls. Additionally managers are to ensure that monthly checks are undertaken and supported by Service Managers annual inspections.

13. Exclusions to the Policy

The Security Policy encompasses the physical environment and protection of NHS property and personal safety to patients and staff. There are a number of security related areas which due the specialised nature are subject to their own

Policy/Procedure and are therefore excluded from this Policy/Procedure these areas are listed below.

13.1 CCTV

Closed circuit television systems is in operation in the Gilbert Bain Hospital and is subject to the CCTV Protocol.

13.2 Health Records

Patient's health records in all forms (electronic, paper or other media) are highly confidential and sensitive documents and the management of them is subject to legislation. Managers are to ensure that the security measures are in place in accordance with; the Patient Confidentiality Policy and the **Access to Health Records Act 1990,** and the **Data Protection Act 1998** and the **Medical Records Act 1988.**

13.3 Information Governance

The security of information in an electronic or a hard copy format is subject to the Information Security Policy

13.4 Lone Working

There are many and varying risks presented to the Lone and Peripatetic Workers who by course of their working routine may be required to work by themselves for significant periods of time without close or direct supervision and are subject to the Lone Worker Policy

13.5 Major Emergency Incidents

Links to the following major emergency topics:

- Major Emergency Response; Major Emergency Response Plan

13.6 Management of Violence and Aggression

Security incidents will include acts violence and aggression and are to be reported. The Management of Violence and Aggression Policy provides management and staff guidance in relation to behaviours which may arise through a range of security related issues.

- Management of Violence and Aggression Policy
- Guidelines for the use of Physical Intervention
- Guidelines for the use of Restraint

13.7 Missing Patient/Lost Persons

Individual Wards/Departments/Units have the responsibility for the management of their missing patients and therefore should have procedures in place.

The procedure below details action to be taken by Staff in locating and reporting the whereabouts of a missing patient.

13.8 NHS Fraud

Financial management of NHS SHETLAND monies is subject to Shetland NHS Board Standing Financial Instructions (SFI's) and Financial Operating Procedures (FOP's)

14. Review of Policy

A review of this policy will be undertaken every Three years or sooner should future security and safety developments indicate. All changes will be brought to the attention of employees.

References:

Managing Health at Work Partnership Information Network (PIN)
Guideline, Scottish Government ,2003 can be found here:
http://www.gov.scot/Publications/2003/02/16388/18311

Good practice statement on the prevention and management of violence
Clinical Research and Audit Group, 1996. Can be found here
http://www.gov.scot/Resource/Doc/46951/0013967.pdf