

# SECURITY MANAGEMENT

## STANDARD

**There is a secure environment that protects all service users, staff and visitors and their property, and the physical assets of the organisation.**

## OVERVIEW

All HSC organisations should be committed to providing a safe and secure environment for staff, patients and visitors, framed by National and European Health and Safety Legislation, by DHSSPSNI Policy and by their common law duty of care. Whilst security management in HSC organisations is the responsibility of senior management, security itself is everyone's responsibility. Security involves all groups of staff at all levels, and to be effective it is important to establish at the outset the support of everyone in the organisation. Sensible and cost-effective security management initiatives can be taken to reduce risks to all stakeholders by establishing a culture that aims to prevent all criminal activity. In order to develop appropriate policies and procedures regarding security, co-operation and collaboration with other parties is essential (i.e. other organisations who may use the site; local police etc).

## KEY REFERENCES

British Standards Institution *The Code of Practice for Security Screening of Personnel Employed in a Security Environment*. BS7858.BSI, London.

Northern Ireland (1997) *The Protection from Harassment (Northern Ireland) Order 1997* (S.I.1997/1180 (NI.9)) The Stationery Office.

UK (2000) *The Regulation of Investigatory Powers Act 2000* (c.23) The Stationery Office.

Northern Ireland (1999) *Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (Northern Ireland) (RIDDOR) 1997*. (SR&O 1997No.455) The Stationery Office.

Local government information unit *A watching brief, A code of practice for CCTV*.

National Association for Healthcare Security (1997) *The Basic Training Manual and Study Guide* N.A.H.S. 1997 (this document is available free of charge to all members of the National Association for Healthcare Security (N.A.H.S.) on request to [enquiries@nahs.org.uk](mailto:enquiries@nahs.org.uk)).

The Health & Safety at Work (Northern Ireland) Order 1978

Public Order (NI) Act 1987

DHSSPSNI 2000 Campaign to Stop Violence Against Staff Working in the NHS HSS (GEN 1)5/2000

DHSSPSNI 2003 Campaign to Stop Violence Against Staff Working in the HPSS HSS (Gen 1) 3/2003

Zero Tolerance On Abuse Of Staff: Protecting Healthcare And Emergency Staff From Violence; **HSS (GEN) (3) 2007**

NHS Executive (1999) *Clinical Governance in the New NHS*. HSC 1999/065. 1999.

NHS Executive (1999) *Governance in the New NHS. Controls Assurance Statements 1999/2000 Risk Management and Organisational Controls*. HSC 1999/123. 1999.

NHS Executive (2001) *Governance in the New NHS: Controls Assurance Statements 2000/2001 and Establishment of the Controls Assurance Support Unit*. HSC 2001/005. 2001

NHS Executive (1999) *Guidelines for Implementing Controls Assurance in the NHS: Guidance for Directors*. NHS Executive, London

*Standards Australia (2004) Risk Management AS / NZS 4360:2004. Standards Association of Australia. Strathfield NSW.*

HSS (PPM) 3/2002 Corporate Governance: Statement on Internal Control

HSS (PPM) 4/2005 AS/NZS 4360: 2004 – Risk Management

HSS (PPM) 8/2002 Risk Management in the Health and Personal Social Services

HSS (PPM) 10/2002 Governance in the HPSS – Clinical and Social Care  
Governance: Guidelines for Implementation

HSS (PPM) 13/2002 Governance in the HPSS: Risk Management

HSS (PPM) 5/2003 Governance in the HPSS: Risk Management and Controls  
Assurance

HSS (PPM) 6/2004 Reporting and Follow-up on Serious Adverse Incidents: Interim  
Guidance

HSS (PPM) 8/2004 Governance in the HPSS: Controls Assurance Standards –  
Update

#### **OTHER PUBLICATIONS**

NHS Executive (1997) *Effective management of security in A&E* NHS Executive,  
London

NHS Executive (1993) *Hospital Security* EL (93) 47 NHS Executive, London

NHS Executive (1992) *NHS Security Manual* National Association of Health  
Authorities and Trusts.

NHS Executive (1995) *Safe and Sound: Security in NHS maternity units* NHS  
Executive, London.

NHS Executive (1997) *Security in the NHS* EL (96) 13 NHS Executive, London.

Emergency Workers (Scotland) Act 2005

Emergency Workers (Obstruction) Act 2006

## CRITERION 1

**Board level responsibility for security is clearly defined and there are clear lines of accountability for security management throughout the organisation, leading to the Board.**

### INFORMATION

#### Source

- NHS Executive (1999) *Clinical Governance in the New NHS*. HSC 1999/065. 1999
- NHS Executive (1999) *Governance in the New NHS. Controls Assurance Statements 1999/2000 Risk Management and Organisational Controls*. HSC 1999/123. 1999.
- Standards Australia (2004) *Risk Management AS / NZS 4360:2004*. Standards Association of Australia. Strathfield NSW.
- HSS (GEN)(3) 2007, Zero Tolerance On Abuse Of Staff: Protecting Healthcare And Emergency Staff From Violence;

#### Guidance

The Chief Executive of the organisation has the overall statutory responsibility for security management within the organisation. An executive director is accountable for controlling and co-ordinating security. In practice, some tasks will be delegated and in many organisations a security specialist is employed. Many managers have a direct responsibility for security e.g. nurse managers, estate managers, etc. Individual responsibility and duties should be clearly defined, with specialist training given.

An annual security report should be submitted to the Board. The report should include statistics and performance in meeting agreed objectives e.g. crime prevention.

#### Examples of Verification

- Accountability arrangements chart
- Minutes of Security Committee/Forum
- Board minutes

#### Links with other standards

All standards (generic criterion)

## CRITERION 2

**There is a Board-approved robust Zero Tolerance and security policy and strategy that is fit for purpose and has been communicated throughout the organisation supported, where appropriate, by agreed plans.**

### INFORMATION

#### Source

- DHSSPSNI 2000 Campaign to Stop Violence Against Staff Working in the NHS HSS (GEN 1)5/2000
- DHSSPSNI 2003 Campaign to Stop Violence Against Staff Working in the HPSS HSS (Gen 1) 3/2003
- HSS (GEN)(3) 2007, Zero Tolerance On Abuse Of Staff: Protecting Healthcare And Emergency Staff From Violence;

#### Guidance

All health organisations are required to adopt formal security policy and strategy and to have clear implementation plans, which should be communicated to the relevant stakeholders.

Specifically, the policy and strategy should;

- Set out the intentions of the policy and strategy and the management commitment to it
- State exactly what the objectives are e.g., this employer supports a Zero Tolerance approach to Violence against staff
- Identify how security risks will be assessed
- Address how specific risks will be tackled e.g. violence and aggression
- Identify how the policy and strategy will be communicated to relevant stakeholders
- Set out the security responsibilities of individuals and groups of staff e.g. appoint a Senior Director with responsibility for staff safety.
- State how security fits with other organisational functions such as health and safety, fire safety and internal audit
- Identify where staff can go for advice on security and violence matters.
- Ensure that formal procedures are in place to ensure that risks to staff are continuously monitored, reviewed and managed.
- Ensure key indicators capable of showing the effectiveness of the policy are in place and regularly review to ensure the efficacy and usefulness of the indicators.
- To work in partnership with other organisations to develop a common understanding of how best to deal with attackers e.g. PSNI, Criminal Justice Agency

The security strategy should look to the future and contain robust crime reduction objectives.

Where appropriate, the policy and strategy should include requirements for sensitive and/or high-risk areas.

#### Examples of Verification

- Policy/strategy document
- Board minutes indicating adoption
- Documented security plan.

#### Links with other standards

None (D/N does this link to Health and Safety Standard?)

## CRITERION 3

**A crime prevention programme is implemented and supported throughout the organisation.**

### INFORMATION

#### Source

- DHSSPSNI 2000 Campaign to Stop Violence Against Staff Working in the NHS HSS (GEN 1)5/2000
- DHSSPSNI 2003 Campaign to Stop Violence Against Staff Working in the HPSS HSS (Gen 1) 3/2003
- HSS (GEN)(3) 2007, Zero Tolerance On Abuse Of Staff: Protecting Healthcare And Emergency Staff From Violence;

#### Guidance

Crime prevention is the cornerstone of a security strategy.

All staff should be involved in crime prevention and security. Good practice suggests induction and on-going training should include:

- Awareness of the crime problems
- What is being done to reduce crime
- How best to protect patients and staff
- How best to guard against assault and theft of personal belongings
- What they are expected to do to safeguard property belonging to patients
- When, and in what circumstances, staff may have to call the police

#### Examples of Verification

- Training records
- Training course material

#### Links with other standards

None

## CRITERION 4

**There is proper and timely response to security incidents in accordance with appropriate response plans for specific security incidents.**

### INFORMATION

#### Source

- DHSSPSNI 2000 Campaign to Stop Violence Against Staff Working in the NHS HSS (GEN 1)5/2000
- DHSSPSNI 2003 Campaign to Stop Violence Against Staff Working in the HPSS HSS (Gen 1) 3/2003
- HSS (GEN)(3) 2007, Zero Tolerance On Abuse Of Staff: Protecting Healthcare And Emergency Staff From Violence;
- 

#### Guidance

The key to limiting the impact of any security-related incident is for any person who has responsibility to respond to be adequately trained. However, in order to ensure that timely and effective response is possible, there must be a system in place.

Good security response plans should be based on the following principles:

- Deter criminal activity where possible
- Deny the criminal the opportunity and delay the attack if it happens
- Detect incidents when they happen and respond effectively.
- Response plans should be so designed as to be able to react to any security incident.

There should be a follow-up procedure that offers, as appropriate, media support, counselling, loss analysis, prosecution/disciplinary action and review/feedback reports.

#### Examples of Verification

- Documented security incident response plans
- Documented reports on handling of actual security incidents
- Training records

#### Links with other standards

None

## CRITERION 5

**Security hazards and incidents are reported and analysed in accordance with the processes contained in the Risk Management standard.**

### INFORMATION

#### Source

- Northern Ireland (1997) *Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) (Northern Ireland) 1997 (SR&O 1997 No.455)*. The Stationery Office.
- DHSSPSNI 2000 Campaign to Stop Violence Against Staff Working in the NHS HSS (GEN 1)5/2000
- DHSSPSNI 2003 Campaign to Stop Violence Against Staff Working in the HPSS HSS (Gen 1) 3/2003
- HSS (GEN)(3) 2007, Zero Tolerance On Abuse Of Staff: Protecting Healthcare And Emergency Staff From Violence;

#### Guidance

An effective hazard/incident reporting system will help organisations identify problem areas where incidents are frequently arising and will help organisations to conduct robust risk assessments.

An incident can be defined as any event, which has given or may give rise to actual or possible personal injury, or to property loss or damage. This definition covers all security incidents.

The following are the salient requirements of a hazard and incident reporting system for security purposes:

- All incidents graded by severity
- Investigations of more serious incidents carried out to determine underlying cause
- All incidents should be analysed to establish underlying trends
- Regular management reports should be produced which result in management action
- Preferably uses one form for reporting all incidents

None of the above alters the requirement to report hazards/incidents under RIDDOR.

#### Examples of Verification

- Completed incident report forms
- Copies of RIDDOR report forms
- Incident reporting procedure
- Incident management procedure
- Incident software

#### Links with other standards

Risk Management  
Health and Safety Management

## CRITERION 6

**The risk management process contained within the Risk Management standard is applied to security risks.**

### INFORMATION

#### Source

- Standards Australia (2004) *Risk Management AS / NZS 4360:2004*. Standards Association of Australia. Strathfield NSW.

#### Guidance

Security risks should be systematically identified and recorded on a continuous basis. Risks can be systematically identified using a number of approaches including:

- Review of inspection/audit reports
- Workshops with staff
- Use of compliance checklists
- Risk assessments

The following risk management elements should be in place:

- All identified risks should be documented as part of a 'risk register' and should be systematically analysed and prioritised for action.
- Risk treatment plans should be developed and implemented (in order of priority and alongside other risk treatments which are necessary to deal with wider risks faced by the organisation, where appropriate) in order to minimise risk.
- Risks and the effectiveness of implemented risk treatments should be monitored and reviewed on a continuous basis.
- Senior management and the Board should be informed of any significant risks and associated risk treatment plans.
- All relevant staff, including those on fixed term contracts, and other relevant stakeholders should receive information on systems in place to minimise security risks.
- Where appropriate, staff training should be undertaken to reduce knowledge gaps.

#### Examples of Verification

- Risk Register
- Risk treatment plans
- Staff training/information log
- Correspondence with stakeholders

#### Links to other standards

Risk Management

## CRITERION 7

**The organisation has access to up-to-date security-related legislation and guidance.**

### INFORMATION

#### Source

#### Guidance

Access to legislation and guidance is essential for the organisation to carry out the statutory duties imposed upon it by law and mandatory duties imposed by the Department.

As a minimum, the organisation should have access to the key references listed on the front page of this standard, together with any additional references noted in the guidance associated with the criteria contained in this standard.

There are many sources of information on legislation and fire safety guidance, including books and, through subscriptions to specialist information providers, CD-ROMs containing the full text. Up-to-date guidance can be accessed on the Internet on the Department of Health COIN database (<http://www.doh.gov.uk>). The Health and Safety Executive's website (<http://www.hse.gov.uk>) contains up-to-date information on legislation and guidance. Full text copies of all legislation issued from 1 January 1997 can be downloaded from (<http://www.official-documents.co.uk>) which contains information on UK official documents. . Information from the National Association for Healthcare Security website can be downloaded at <http://www.nahs.org.uk>.

#### Examples of Verification

- Library
- CD-ROMs
- Internet access

#### Links with other standards

All standards (generic criterion)

## CRITERION 8

**All employees receive security training that is commensurate with risks in their work area.**

### INFORMATION

#### Source

- National Association for Healthcare Security (1997) *The Basic Training Manual and Study Guide* N.A.H.S. 1997
- DHSSPSNI 2000 Campaign to Stop Violence Against Staff Working in the NHS HSS(GEN 1)5/2000
- DHSSPSNI 2003 Campaign to Stop Violence Against Staff Working in the HPSS HSS (Gen 1) 3/2003
- HSS (GEN)(3) 2007, Zero Tolerance On Abuse Of Staff: Protecting Healthcare And Emergency Staff From Violence;

#### Guidance

Training is the essential foundation for reducing risk to personnel safety and for crime prevention. Thus, security awareness training should be part of the overall training profile for all HPSS staff.

Training needs to be targeted to all levels of the organisation to have the maximum benefit. However, not every staff member needs the same training. Security training needs should be based upon the risk that a given employee will experience a security incident in his or her work area, based on historical data and other factors, including the results of detailed risk assessments.

For example, special security training will most likely need to be provided in maternity, A&E and children's services, where there is known to be heightened risk at the point of care.

At a minimum, security training should cover areas such as:

- Crime prevention practices
- Security response procedures (proper and timely response duties by staff)
- Use and maintenance of security equipment.
- Customer care training for frontline staff
- Recognising signs of aggression
- Dealing with verbal abuse and violence.

#### Examples of Verification

- Training logs
- Training material

#### Links with other standards

Human Resources

## CRITERION 9

**The competency and performance of security personnel, whether employed internally or out-sourced, is monitored to ensure that a high standard is maintained**

### INFORMATION

#### Source

- British Standards Institution *The Code of Practice for Security Screening of Personnel Employed in a Security Environment*. BS7858. London, BSI
- National Association for Healthcare Security (1997) *The Basic Training Manual and Study Guide* N.A.H.S. 1997

#### Guidance

There should be adequate screening and training procedures in place for the security staff who are employed by the organisation. Security staff should have terms and conditions of employment that are compliant with the Working Time Regulations (e.g. a 48-hour week averaged over 17 weeks).

In accordance with personnel policies, clear instructions on actions to be taken for all possible events should be available, and security personnel should be fully and appropriately trained to perform their duties. For example, security staff must clearly understand their powers of arrest.

The competency and performance expectations for security staff should be assessed and determined for each organisation. Security staff should then be evaluated against competency requirements and performance expectations.

If an external contractor is employed to provide security services, the service contract should clearly set out:

- Screening procedures for all staff
- Compliance with the working time directive
- Uniform requirements
- Duties and response to incidents
- Training standards
- Equipment requirements
- Performance monitoring and record keeping
- Call out procedures
- Liaison with local police

#### Examples of Verification

- Monitoring arrangements
- Training course material
- Screening documentation

#### Links with other standards

Human Resources

## CRITERION 10

**Key indicators capable of showing improvements in security management, and the management of associated risks, are used at all levels of the organisation, including the Board, and the efficacy and usefulness of the indicators is reviewed regularly.**

### INFORMATION

#### Source

- HSS (PPM) 10/2002 – Governance in the HPSS: Clinical and Social Care Governance – Guidance on Implementation
- DAO (DFP) 5/2001 – Corporate Governance: Statement on Internal Control, and
- HSS (PPM) 3/2002 – Corporate Governance: Statement on Internal Control
- DAO (DFP) 25/2003 – Statement of Internal Control

#### Guidance

The organisation should develop indicators that demonstrate the risks associated with security management within the organisation. One indicator is degree of compliance with this standard. Ideally the indicators should be designed to demonstrate improvement in the risks associated with security management over time. The number of indicators devised should be sufficient to monitor the security management service and the risk management process. It is not necessarily the case that the Board will use all the indicators. The Board should select those that are useful for ensuring that the internal controls are working satisfactorily and security management services are meeting their objectives.

The Department will review the actual indicators used by organisations to identify best practice in indicator use. This will inform the development of a set of national indicators for benchmarking and monitoring purposes.

#### Examples of Verification

- Indicators
- Evidence of usage at all levels

#### Links with other standards

All standards (generic criterion)

## CRITERION 11

**The system in place for managing security is monitored and reviewed by management and the Board in order to make improvements to the system.**

### INFORMATION

#### Source

- HSS (PPM) 10/2002 – Governance in the HPSS: Clinical and Social Care Governance – Guidance on Implementation
- DAO (DFP) 5/2001 – Corporate Governance: Statement on Internal Control, and
- HSS (PPM) 3/2002 – Corporate Governance: Statement on Internal Control
- DAO (DFP) 25/2003 – Statement of Internal Control

#### Guidance

It is the responsibility of the Chief Executive and the Board to monitor and review all aspects of the security management system, including:

- Accountability arrangements
- Processes, including risk management arrangements
- Capability
- Outcomes
- Internal audit findings

In some organisations, a specialist security committee or group may review the detailed issues surrounding the management of security risks. The Risk Management Committee may play a significant role in monitoring and reviewing all aspects of the system as a basis for establishing significant information that should be presented to, and dealt with by the Board. The Health and Safety Committee may also play a significant role in reviewing aspects of security. The Audit Committee should review internal audit findings.

#### Examples of Verification

- Internal audit report(s)
- Specialist security committee/group minutes
- Audit Committee minutes
- Risk Management Committee minutes
- Health and Safety Committee minutes

#### Links with other standards

All standards (generic criterion)

## CRITERION 12

**The Board seeks independent assurance that an appropriate and effective system of managing security is in place and that the necessary level of controls and monitoring are being implemented.**

### INFORMATION

#### Source

- NHS Executive (1999) *Guidelines for Implementing Controls Assurance in the NHS: Guidance for Directors*. NHS Executive, London
- NHS Executive (1995) *NHS Internal Audit Manual 1995*. NHS Executive, London.

#### Guidance

Management should consider the range of independent internal and external assurance available, and avoid duplication and omission.

The adequacy of the independent assurance will depend upon the scope and depth of the work performed, bearing in mind its timeliness and the competency of the staff performing it. The level of reliance that can be placed upon such assurances should consider, among other things, the professional standing of the assurer, their level of independence, and whether they could reasonably expect to provide an objective opinion. It is important that any review that takes place results in a report, recommendations for action where necessary, and the retention of sufficient evidence to enable other potential reviewers to rely upon the work already undertaken. The reports should be made to the appropriate sub-committee of the Board.

Management arrangements will include an internal audit function, as well as other quality control and assurance functions such as clinical audit. The internal audit function is required to give an opinion to the Board on the adequacy and effectiveness of the overall system of internal control. In doing so, they will seek to work with, and rely on the work of, other review bodies as far as is practical. The HPSS is given external assurance by such bodies as:

- External auditors, as appointed by the Audit Commission
- Commission for Health Improvement

More specific assurance for this standard may be gained from visits by any regulatory body approved by the Security Industry Authority.

#### Examples of Verification

- Schedule of planned reviews
- Copy of reports
- Committee minutes
- Action plans
- Notes of follow up of actions
- Evidence file
- Details of staff involved in the review.

#### Links with other standards

All standards (generic criterion)