HSC Northern Ireland Ambulance Service
Health and Social Care Trust

NORTHERN IRELAND
AMBULANCE SERVICE

SECURITY POLICY

April 2014

Version 2.0

HSC Northern Ireland Ambulance Service
Health and Social Care Trust

N.I.A.S.

Title:	**Security Policy**		
Purpose of Policy:	To set out NIAS policy on Security across the Trust in all its activities.		
Directorate Responsible for Policy:	Operations		
Name and Title of Author:	Bryan Snoddy, Assistant Director of Operations		
Staff Side Consultation	11/10/2011 for consideration		
Equality Screened:	21/07/11		
Date Presented to:	SEMT	13 Sept 2011 & 18 Oct 2011	
	Assurance Comm	12 March 2012	
	Trust Board	**17 November 2011**	
Publication Date:		Review Due: 12 March 2013	Review completed: 2/04/2014
Version:	**Version 1.3** Minor amendments required by Trust Board. Assurance Committee confirmed changes on 12 March 2012.		
(01)	**Version 2.0** Circulated for review in NIAS. No amendments as at 2/04/2014		
(02)			

Circulation List:

This Policy was circulated to the following groups for consultation.

- Staffside
- Executive Directors and Senior Managers

Following approval, this policy document was circulated to the following staff and groups of staff.

- All Trust Staff
- Trust Internet Site/ Intranet Site

Contents Page Number

1.0 Introduction

1.1 This policy sets out the Northern Ireland Ambulance Service Health and Social Care Trust's (hereafter referred to as 'The Trust') plan for the management of Security.

1.2 The policy identifies the Trust's commitment to the management of Security in all its activities.

1.3 This policy gives guidance on reporting and managing security including: incident investigation, minimising risk and promoting a culture of continuous improvement.

1.4 The policy should be read in conjunction with the Trust's procedural arrangements for Security.

1.5 This policy has been developed in consultation with internal stakeholders.

2.0 Policy Statement

2.1 The Trust promotes a pro-active approach to the management of Security.

2.2 The Trust will endeavour to minimise risks to patients, service users, clients, staff, visitors, contractors and others through the effective management of Security.

2.3 The Trust recognises that breaches of security in any of its forms could have a significant impact, not only on its staff and physical assets, but also on public confidence and the morale of staff and patients.

2.4 The Trust is committed to providing a safe and secure environment for its staff, patients and visitors as outlined by National and European Health and Safety Legislation and directives, by DHSSPSNI Policy and by common law duty of care.

3.0 Definitions

3.1 This Security policy will cover any event which has given or may give rise to actual or possible personal injury or to property loss or damage.

3.2 The term “security” will apply to the elimination or reduction of the risk of crime in all its forms within the Trust and will, for example, apply to:

- Crimes against individuals – violence and abuse;
- Crimes to and theft from premises or vehicles;
- Theft or misappropriation of drugs;
- Security of IT hardware and peripherals;

4.0 Scope of the Policy

4.1 This Policy applies to all sites and vehicles across the Trust.

4.2 This policy should be read in conjunction with any strategies, other policies and procedures covering any aspect of security in the Trust.

4.3 It must be adhered to by all Trust employees. It will also apply to those who carry out work for the Trust such as contractors and agency staff. It includes a commitment to the continual improvement of security and to comply with legal and other requirements.

4.4 A number of specific policies and procedures exist, within the Trust, which relate to the security of Trust premises, staff, vehicles, equipment. In addition there are specific policies and procedures in place relating to fraud and information. All issues in relation to fraud falling under the Fraud Policy must be reported to the Trust Fraud Officer and through to the Audit Committee.

The Trust’s ICT Security Policy (2009) and Data Protection 1998 Policy (2009) outline staff responsibilities and processes for reporting breaches of information security. (See Appendix 1 for list of relevant policies and documents)

5.0 **Policy Objectives**

5.1 To ensure that the Trust has in place suitable and robust governance arrangements to support the management of Security.

5.2 To define Board level responsibility for security management and show that there are clear lines of accountability throughout the Trust leading to the Board.

5.3 To ensure there are resources to support the management and the development of processes and systems associated with security management.

5.4 To ensure compliance with relevant legislation and that the Trust has access to up-to-date security related legislation and guidance.

5.5 To support the development of appropriate systems and processes to monitor and review security management.

6.0 Roles and Responsibilities

6.1 The Chief Executive has overall responsibility for Security Management within the Trust. Together with the Trust Board, the Chief Executive ensures that the objectives of this policy are met.

The Chief Executive delegates the day to day responsibility for establishing and monitoring the implementation of this policy to Directors.

The Chief Executive is responsible for ensuring periodic review of the Trust's Security Policy.

6.2 The Director of Finance is the designated Executive Director with lead responsibility for finance, fraud and information security. There are specific policies and procedures for dealing with these issues (see Appendix 1) and staff should refer to these for further detailed guidance. Security issues relating to finance, fraud and information will be dealt with through the Audit Committee.

6.3 The Director of Operations is the designated Executive Director with lead responsibility for general Security Management. There are relevant policies and procedures for dealing with these issues (see Appendix 1) and staff should refer to these for further detailed guidance. Security issues relating to general Security Management will be dealt with through the Assurance Committee.

6.4 The Assistant Director of Operations has responsibility for reviewing this Security Policy and associated procedures and for providing advice to the Trust on general security matters within this remit.

6.5 All NIAS Trust Directors, Assistant Directors and Senior Managers have a responsibility for ensuring they have a comprehensive understanding of their own remit within the Trust's Security Policies and any associated procedures and that:

- Security risks within their area are identified, reported and documented using a risk assessment approach in line with the Trust's Risk Management Strategy, i.e. Untoward Incident Reporting system.

- Adequate and suitable security measures are implemented to maintain the security of their area of responsibility including the safety of patients, staff, visitors and the safeguarding of Trust assets i.e. equipment and supplies.

6.6 All Trust staff have a responsibility to adhere to this policy and ensure that they operate in accordance with its supporting procedural arrangements.

6.7 It is the duty of all staff to be vigilant and promptly report any security incidents or suspicious circumstances to their line managers. All employees have a responsibility to safeguard themselves and the security of Trust assets.

6.8 Trust appointed contractors must comply with this policy and meet legal and statutory requirements.

7.0 Risk Management

7.1 Significant security risks within the Trust will be assessed in accordance with the Management of Health and Safety at Work (Regulations) Northern Ireland 2006 and the Trust Risk Management Strategy.

7.2 Sensitive or high risk issues will be managed by the risk owner and monitored by the Facilities and Support Group.

7.3 The Untoward Incident reporting procedure will be used to report any security related events. This will allow the Trust to be informed of the risks facing the organisation and to take appropriate action to avoid, minimise or significantly reduce the occurrence or repetition of these incidents.

7.4 A procedure will be developed to ensure that any security incident is followed up appropriately. i.e. Finance, fraud and information security issues will be investigated as advised by the Director of Finance and general security issues will be investigated as advised by the Director of Operations.

7.4 These incidents will be monitored and reviewed by the Facilities & Support Group and reported through to the Assurance Committee. (See Appendix 2 for the Committee Structure)

7.5 Staff should participate in any security related training and should be able to respond in an appropriate manner.

7.6 Security arrangements and the effectiveness of policy and procedures will be reported to the Assurance Committee and monitored through the Facilities & Support Group.

8.0 Equality and Human Rights Considerations

8.1 This policy has been screened for equality implications as required by Section 75, Schedule 9, of the Northern Ireland Act, 1998. Equality Commission for Northern Ireland guidance states that the purpose of screening is to identify those policies which are likely to have a significant impact on equality of opportunity so that greatest resources can be targeted at them.

8.2 This policy has also been considered under the terms of the Human Rights Act, 1998, and was deemed to be compatible with the European Convention Rights contained in that Act.

8.3 This policy embraces Diversity, Dignity and Inclusion in line with emerging Human Rights guidance. We recognise, acknowledge and value difference across all people and their backgrounds. We will treat everyone with courtesy and consideration and ensure that no-one is belittled, excluded or disadvantaged in any way, shape or form.

8.4 Using the Equality Commission’s screening criteria; no significant equality implications have been identified. This Policy will therefore not be subject to an equality impact assessment.

8.5 This Policy will be included in the Trust’s register of screening documentation and maintained for inspection whilst it remains in force.

8.6 This document can be made available on request in alternative formats, e.g. Braille, disc, audio cassette and in other languages to meet the needs of those who are not fluent in English.

9.0 Policy Review

9.1 The Trust is committed to ensuring that all policies are kept under review to ensure that they remain compliant with relevant legislation.

9.2 This policy will be reviewed by the Assistant Director of Operations at two yearly intervals or following a high risk incident. It will also be reviewed subject to any relevant European directives or legislation. Any review will be noted on a subsequent version of this policy, even where there are no substantive changes made or required.

10.0 Legal and Statutory requirements

10.1 Legislative compliance, relevant policies, procedures, statutes, guidance, circulars and other publications relevant to this policy are listed in the HPSS Controls Assurance Standard (CAS) for Security management. The relevant CAS can be located at the DHSSPSNI website under 'Governance in the HPSS' at the current link below: -

http://www.dhsspsni.gov.uk/index/hss/governance/governance-controls.htm

NIAS policies and procedures can be found using the NIAS intranet link below: -

http://nias-sharepoint:81/policies_procedures/policy.htm

10.2 Other relevant documents, legislation, statute and guidance can be found at Appendix 1. Relevant related documents can also be found by following the links supplied above to the DHSSPSNI and NIAS websites and intranet.

Appendix 1

Related relevant documents

- Health and Safety at Work (Regulations) Northern Ireland 2006
- ICT Security Policy 2009
- Data Protection Act 1998 Policy (2009)
- Records Management Policy (2009) and associated guidance
- Trust Risk Management Strategy (An Assurance Framework) 2009-2013
- Untoward Incident Reporting Procedure 2009
- Fraud Policy 2010
- Lone Workers Policy (Annual Report)

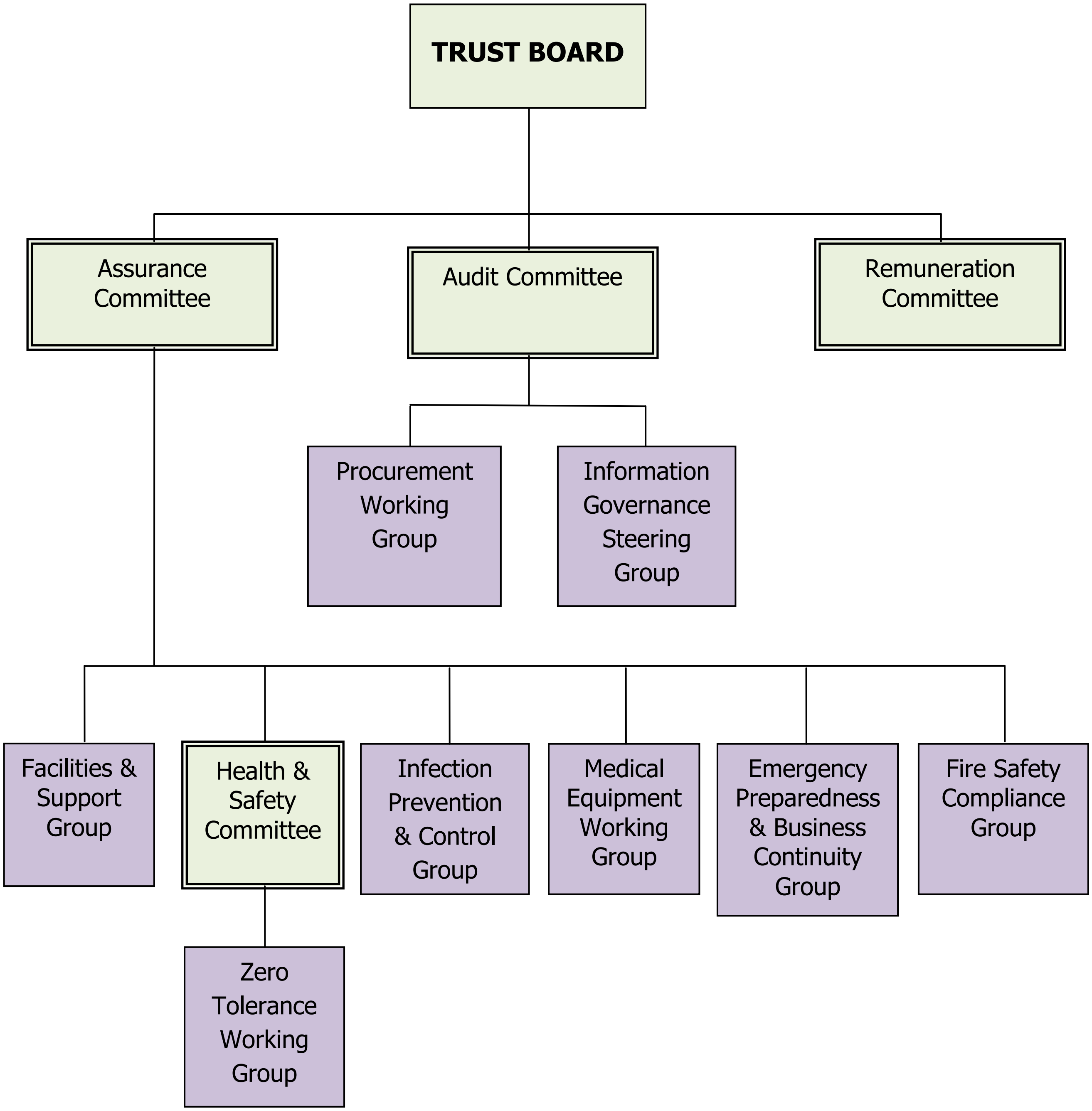
Finance and ICT related documents

- Fraud Policy (2008 revised Nov 2009)
- Fraud Reporting Guide (HSC
- National Fraud Initiative (NFI) – Quarterly notification of fraud cases.
- Revised Fraud Reporting Arrangements for HSC Bodies (HSSPSNI Sept 2011)
- Information and Communications Technology (ICT) Policy (2009)

This list is not exhaustive and other documents can be found by following the links supplied above to the DHSSPSNI and NIAS websites and intranet.

Appendix 2

Committee and Group Structure


TRUST BOARD
Assurance Committee
Audit Committee
Remuneration Committee
Procurement Working Group
Information Governance Steering Group
Facilities & Support Group
Health & Safety Committee
Infection Prevention & Control Group
Medical Equipment Working Group
Emergency Preparedness & Business Continuity Group
Fire Safety Compliance Group
Zero Tolerance Working Group