Western Health and Social Care Trust

ZERO TOLERANCE AND SECURITY POLICY

September 2015

Policy Title	ZERO TOLERANCE AND SECURITY POLICY
Policy Reference Number	Corp10/01
Implementation Date	December 2009
Revised Date	February 2013
Revised Date	September 2015
Review Date	September 2017
Responsible Officer	Maureen Kelly Head of Patient and Client Support Services

Table of Contents

1.0 POLICY STATEMENT

1.1 The Trust recognises its responsibilities to provide a secure environment that protects patients, clients, staff and visitors and their property and the assets of the organisation.

1.2 The management and implementation of the Trust's security arrangements will be a key element of the Trust's Risk Management and Health & Safety programmes and action plans as well as the Department of Health, Social Services and Public Safety Circular HSS (GEM) (3) 2007 Zero Tolerance on Abuse of Staff protecting healthcare and emergency staff from violence.

1.3 The Trust Board is committed to providing the resources and support systems necessary to ensure its responsibilities are seen to be discharged as far as is reasonably practicable and will make provision for the management, organisation and implementation of security arrangements within the Trust.

2.0 INTRODUCTION

2.1 This document outlines how the Western Health and Social Care Trust will ensure that there is a safe and secure environment that protects patients, clients, staff and visitors as well as the assets of the Trust.

2.2 This policy puts into effect the Trusts approach to the management of security in the Trust and outlines the new requirements that will apply from the implementation of the Controls Assurance Standards, to ensure the highest possible professional standards are implemented. Also the policy will seek to build on good practice where it exists and ensure that every part of the Trust has access to the skills needed to lead this work effectively.

2.3 This policy's main purpose is to support the development of a safe environment for those who use or work in the Trust that is properly secure so that the highest possible standard of care can be made available to patients and clients. A key role of security management in the Trust is to ensure that patients and clients can enjoy their rights to healthcare while living up to their responsibility to respect and value a service, on which they can rely.

2.4 Managers are responsible for developing local security procedures to meet security requirements of their specific areas of responsibility, resulting from their risk assessments.

2.5 This policy will meet the requirements of the Department circular HSS(GEN)(3) 2007 on Zero Tolerance and will supersede the Trust's Zero Tolerance Policy 2007.

2.6 This policy should be read in conjunction with

- The Zero Tolerance Staff Handbook – May 2014
- The Guidelines for Lone Working – February 2015

3.0 DEFINITION

Security management refers to all aspects of security including the safety of patients, clients' staff and visitors, violent and aggressive behaviour, including verbal abuse break-ins, theft and general site security.

4.0 KEY OBJECTIVES

The Trust must ensure that it has in place suitable and robust governance arrangements to support the delivery and maintenance of a safe and secure environment for patients, client's staff and visitors

4.1 Establishment of a Trust Zero Tolerance and Security Working Group:

The group will be multi-disciplinary and will have representation from all Directorates and Trade Unions. The remit of the group is outlined in **(Appendix i)**

4.2 Identify problems by analysis of trends, risks and incidents:

This will be achieved by the analysis of the Trust's reported incidents, and the implementation of risk assessments within all Directorates. The elements to be included within the risk assessment as shown in section 5.0.

4.3 Creating a clear framework for management of risks:

The identification and relative scoring of the risks will provide a formal list of high to low security shortfalls. This ranking will provide the basis to target physical and human resources at the high risk areas. See Trust Risk Management Policy March 2014

4.4 Creating a strong and feasible working structure:

The multi-disciplinary working group will be the collective focus for all security related issues. The Trust Policy on security also defines levels of responsibility throughout the organisation. See section 5.

4.5 Proper and timely response to security incidents:

The Trust must ensure that there is a proper and timely response to security incidents by ensuring they are reported, analysed and monitored in accordance with the Incident reporting procedure November 2014

5.0 ROLES AND RESPONSIBILITIES

The roles and responsibilities of key staff within the Trust are outlined below; the reporting mechanism for security is contained in **Appendix 2**.

5.1 Chief Executive

The Chief Executive as the Accountable Officer has overall responsibility for security management within the Trust. The day to day responsibility will be delegated to the Director of Planning and Performance Management.

5.2 Director of Planning and Performance Management

The Director of Planning and Performance is the designated Director with lead responsibility for Security Management. Director of Planning and Performance will report to Trust Board on matters relating to security management.

5.3 Director of Human Resources

The Director of Human Resources is the designated Director with lead responsibility for Zero Tolerance in relation to physical and verbal abuse

5.4 Assistant Director of Facilities Management

The Assistant Director of Facilities Management is responsible for ensuring Security Management arrangements are in place throughout the Trust. They have responsibility for providing advice to the Director of Performance and services improvement and the Directorate of Human Resources on all aspects of the implementation of the development of relevant security procedures and guidelines of Trust Security Policy.

5.5 Head of Support Services

The Head of Support Services is responsible for:-

- Ensuring that adequate security staff are available, properly trained and competent to perform their duties.
- Ensuring appropriate systems and processes are in place to ensure effective responses to security incidents.
- Act as Chair of the Trust Zero Tolerance and Security Working Group and preparing an annual Zero Tolerance and Security Annual Report.

5.6 Senior Management/Heads of Department

All Trust Directors, Assistant Directors, Heads of Service, Senior Managers, Ward Managers and Heads of Departments and Facilities have responsibility to:-

- Ensure all security risks are identified using the risk assessment approach as outlined in this Security Policy.

- Ensure appropriate security measures are implemented to maintain the security of their area.
- Ensure staff receive security training appropriate to their role and responsibility.
- Ensure all security incidents are reported in accordance with Trust incident reporting procedure.
- Have arrangements in place to ensure all Trust property e.g. ID badges, keys, mobile phones and bleeps are returned by staff in line with Trust Policy when they leave the Trust.
- Ensure all staff within their departments are aware of or receive a copy of the Trust Zero Tolerance Security Policy

5.7 Trust Staff

All staff are required to be aware of the Zero Tolerance and Security Policy and all associated policies procedures and guidelines. It is the duty of all staff to be vigilant, and report any security incident to their line manager. Staff should ensure premises they work in are secured properly and personal property is locked away. Staff should take appropriate action to safeguard Trust property, such as keys, identity badges, documentation etc.

6.0 RISK ASSESMENT

Below are listed those elements deemed relevant to be addressed by the security risk assessment. The list is not exhaustive but reflects the main elements that should be reviewed.

These elements form the basis of the Security Assessment risks **(Appendix iii)**

- Security of Patients & Clients, Staff and Visitors
- Protection of Materials & Equipment
- Property
- Linen Security
- Catering Security
- Medicines Security
- Vehicles & Loads Security
- Road Traffic (Internal)
- The Management of Interpersonal Tensions, Conflict & Aggression
- Bomb Threats & Other Emergencies
- Fraud
- IT Systems Security
- Document Security
- Security of Cash
- Integrated Security Systems

- Physical Security
- CCTV / Alarms / Access
- ID Badges & Security Passes
- Radio Communications
- Security Database
- Bio Chemicals
- Accelerants

Each manager is responsible for carrying out an annual security risk assessment in their area of responsibility, they will identify and prioritise risks and put on appropriate risk registers. Appropriate action plans should be developed for each risk identified with high risks being escalated to either the directorate or corporate risk register as appropriate. Security advice will be provided from Support Services Site Management staff at each Trust location.

7.0 INCIDENT REVIEW/RESPONSE PLAN

All security incidents should be reported using guidance within this Incident Report Procedure November 2014 as described in the Trust's Incident Reporting Policy.

Each department will review all security incidents with specialist security advice from Support Services Site Management Staff.

Security incidents will be reviewed by the Trust Security Working Group, who will review trends by specific incidents and Directorates.

8.0 PREVENTATIVE ETHOS

The ideal outcome of any security Policy is to prevent the security breach before it occurs. This can be achieved in a number of distinctive steps.

8.1 Creating a ***pro-security culture*** amongst staff, professionals and the public to engender a culture where the responsibility for security is accepted by all and the actions of the minority who breach security are not tolerated.

8.2 ***Deterring*** those who may breach security, using publicity to raise awareness of the consequences of their actions, to our patients and clients and the Trust.

8.3 ***Preventing*** security incidents or breaches from occurring, wherever possible, or minimising the risk of them occurring by learning from operational experience about previous incidents, and sharing best practice.

8.4 ***Detecting*** and reporting security incidents or breaches and ensuring these are reported in a simple consistent manner across the Trust to enable trends and risks to be analysed, allowing this data to properly inform the development of preventative measures or the revision of policies and procedures.

8.5 ***Investigating*** and ***Reporting*** security incidents or breaches in a fair, objective and professional manner, to ensure those responsible for such incidents are held to account for their actions and that the causes of such incidents or breaches are fully examined and fed into prevention work to minimise the risk of them occurring again.

8.6 All staff have a vital role to play in protecting themselves including participation in appropriate training and reporting of incidents. The Trust has a responsibility to ensure that appropriate support is given to staff who are victims of a security incident.

8.7 Work in conjunction with relevant bodies e.g. PSNI crime prevention team for advice and guidance on how to prevent security incidents occurring and to assist them in carrying out investigations following breaches of security.

8.8 Security is a fundamental element of the on-going design brief for the Trusts strategic developments. A major factor in the prevention of security incidents is to ensure good design in terms of security at the inception of major building works.

9.0 CONTROLS ASSURANCE

9.1 The controls assurance standard will be the overall quality assurance standard to ensure that the Trust Security Group and the other Trust management functions adhere to the aim of providing a secure environment for patients, clients, staff, visitors and their property.

9.2 The working group will be required to undertake an annual review and scoring of the Controls Assurance standard, prior to signing by the Chief Executive.

10.0 TRAINING

10.1 Responsibility for Zero Tolerance and Security Training is the responsibility of each Directorate and training needs should be developed following each departments Zero Tolerance and Security risk assessment. Training programmes should then be put in place

10.2 More in-depth training will be available to staff with security duties and those at a higher risk of being exposed to aggressive or threatening behaviour.

10.3 All security training is carried out within a professional and ethical framework and adheres to the following principles: -

- **Professionalism**: All staff involved in security shall maintain the highest standards of professionalism, specifically in areas of personal conduct, expertise and all work related to the management of security

- ***Objectivity:*** Security management work should be undertaken with an open mind, particularly in relation to assessment of incidents, evidence or information.

- ***Fairness:*** Respectful approach should be adopted, with an absence of any form of preconception or discrimination in accordance with current human rights legislation.

- ***Expertise:*** All Trust staff with security duties must maintain the highest level of expertise and ensure that this is applied thoroughly and comprehensively.

- ***Propriety:*** Trust staff with security related duties must ensure the highest level of personal integrity. This relates particularly to issues of confidentiality, to ensure information is passed only to those entitled to receive it.

- ***Continuous learning and development*** will be a key objective for all staff but particularly for those staff with front line duties. Training and development will be individually noted on a training record to ensure re-training and further staff development can be planned.

11.0 COMMUNICATION TO STAKEHOLDERS

11.1 The communication of security related issues includes various stakeholders both internal and external and it also involves various levels of detail on each issue.

11.2 Some information is secure and confidential and may be related to potential or ongoing civil or criminal actions. Other information is of a confidential personal nature not for general scrutiny.

11.3 It is important that all staff and other stakeholders particularly members of the public are made aware of the Trust Zero Tolerance approach to physical and verbal abuse of staff.

11.4 Various methods will be employed to support and create a security culture including

- Annual report to the Risk Management Sub-Committee.
- Posters to alert and remind public re Zero Tolerance.
- Induction sessions for new and existing employees.
- P.S.N.I. crime prevention advice.

11.5 This policy will be communicated widely within the Trust with all staff groups and relevant stakeholders

Appendix i

Western Health and Social Care Trust
Trust Zero Tolerance and Security Working Group
Terms of Reference

1. Name of the Group

Trust Zero Tolerance and Security Working Group

2. Membership of the Group

Membership of the group will consist of representatives from

- Medical Services Directorate
- Acute Services Directorate
- Pharmacy
- Primary Care and Older People's Services Directorate
- Adult Mental Health and Disability Services Directorate
- Women and Children's Services Directorate
- Planning and Performance
    - Support Services
    - Estates
- Finance (as required)
- Human Resources (as required)
- Trade Unions/Professional Organisations

3. Quorum

A Quorum will be achieved if the following members of the group are present.

Chair or Deputy Chair plus four other group members

4. Frequency of meeting

Quarterly

5. Record of Meetings

Group meetings will be formally recorded and made available to members as soon as possible after each meeting.

The notes of each meeting shall be formally approved at the following meeting.

6. Accountability of the group

The group will report to the Risk Management Sub-Committee

7. Role and Responsibilities of the Group

- The implementation of the Zero Tolerance and Security Policy and the establishment and implementation of supporting procedures and guidelines.

- The Working Group will provide a focal point for the discussion of all relevant security matters and will work to review/produce security procedures for use throughout the Trust.

- Monitor all security related incidents including violence or aggression towards staff identify trends and develop actions plans to reduce risk.

- To identify the resources required to support the effective management of security and make bids for funding if required.

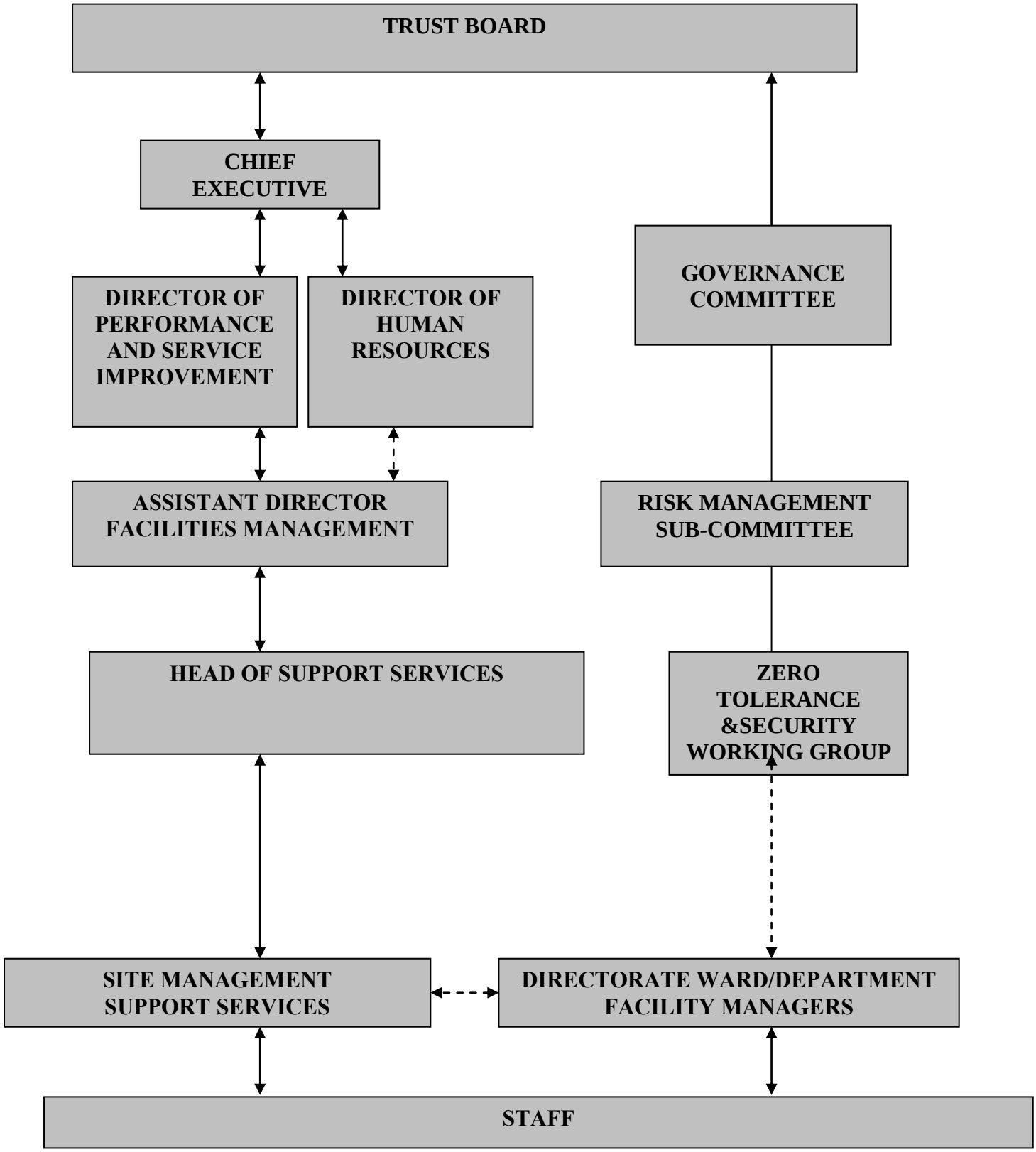
- The Working Group will oversee the arrangements within Directorates for the identification and recording of all security risks and ensuring that Zero Tolerance and Security risks are placed on the appropriate Directorate/Corporate risk register.

- Development of a communication plan to raise general security awareness amongst staff and public.

- Ensure compliance with Security Controls Assurance Standards.

Appendix 2

Governance Reporting Arrangements



DIRECTORATE OF _____- SECURITY RISK ASSESSMENT TEMPLATE **Appendix iii**

Department: _____

Facility: _____

Lead Officer: _____

Assessment carried out by: _____

Risk Element	**Description of Risk** (to be completed for applicable risk elements)	**Risk Rating** (as identified using attached risk matrix scoring method)	**Action Required**	**Action Plan Developed**	**Confirm if included on Directorate / Trust Risk Register**
Security of Patients & Clients, Staff and Visitors					
Protection of Materials & Equipment					
Property					
Linen Security					
Catering Security					
Medicines Security					
Vehicles & Loads Security					
Road Traffic (internal)					
Management of Interpersonal Tensions, Conflict & Aggression					
Bomb Threats & Other Emergencies					
Fraud					

Risk Element	**Description of Risk** (to be completed for applicable risk elements)	**Risk Rating** (as identified using attached risk matrix scoring method)	**Action Required**	**Action Plan Developed**	**Confirm if included on Directorate / Trust Risk Register**
IT Systems Security					
Document Security					
Security of Cash					
Integrated Security Systems					
Physical Security					
CCTV/ Alarms / Access					
ID Badges & Security Passes					
Radio Communications					
Security Database					
Biochemicals					
Accelerants					

NB – This is an indicative list of risk areas and may not include risks particular to your work area. If there are other risk areas, please include them in your risk assessment and add them to this form.

WH&SCT Impact Table – with effect from 1 October 2013

DOMAIN	IMPACT (CONSEQUENCE) LEVELS [can be used for both actual and potential]				
	INSIGNIFICANT (1)	**MINOR (2)**	**MODERATE (3)**	**MAJOR (4)**	**CATASTROPHIC (5)**
PEOPLE *(Impact on the Health/Safety/Welfare of any person affected: e.g. Patient/Service User, Staff, Visitor, Contractor)*	• Near miss, no injury or harm.	• Short-term injury/minor harm requiring first aid/medical treatment. • Minimal injury requiring no/ minimal intervention. • Non-permanent harm lasting less than one month (1-4 day extended stay). • Emotional distress (recovery expected within days or weeks). • Increased patient monitoring	• Semi-permanent harm/disability (physical/emotional injuries/trauma) (Recovery expected within one year). • Increase in length of hospital stay/care provision by 5-14 days.	• Long-term permanent harm/disability (physical/emotional injuries/trauma). • Increase in length of hospital stay/care provision by >14 days.	• Permanent harm/disability (physical/ emotional trauma) to more than one person. • Incident leading to death.
QUALITY & PROFESSIONAL STANDARDS/ GUIDELINES *(Meeting quality/ professional standards/ statutory functions/ responsibilities and Audit Inspections)*	• Minor non-compliance with internal standards, professional standards, policy or protocol. • Audit / Inspection – small number of recommendations which focus on minor quality improvements issues.	• Single failure to meet internal professional standard or follow protocol. • Audit/Inspection – recommendations can be addressed by low level management action.	• Repeated failure to meet internal professional standards or follow protocols. • Audit / Inspection – challenging recommendations that can be addressed by action plan.	• Repeated failure to meet regional/ national standards. • Repeated failure to meet professional standards or failure to meet statutory functions/ responsibilities. • Audit / Inspection – Critical Report.	• Gross failure to meet external/national standards. • Gross failure to meet professional standards or statutory functions/ responsibilities. • Audit / Inspection – Severely Critical Report.
REPUTATION *(Adverse publicity, enquiries from public representatives/media Legal/Statutory Requirements)*	• Local public/political concern. • Local press < 1day coverage. • Informal contact / Potential intervention by Enforcing Authority (e.g. HSENI/NIFRS).	• Local public/political concern. • Extended local press < 7 day coverage with minor effect on public confidence. • Advisory letter from enforcing authority/increased inspection by regulatory authority.	• Regional public/political concern. • Regional/National press < 3 days coverage. Significant effect on public confidence. • Improvement notice/failure to comply notice.	• MLA concern (Questions in Assembly). • Regional / National Media interest >3 days < 7days. Public confidence in the organisation undermined. • Criminal Prosecution. • Prohibition Notice. • Executive Officer dismissed. • External Investigation or Independent Review (eg, Ombudsman). • Major Public Enquiry.	• Full Public Enquiry/Critical PAC Hearing. • Regional and National adverse media publicity > 7 days. • Criminal prosecution – Corporate Manslaughter Act. • Executive Officer fined or imprisoned. • Judicial Review/Public Enquiry.
FINANCE, INFORMATION & ASSETS *(Protect assets of the organisation and avoid loss)*	• Commissioning costs (£) <1m. • Loss of assets due to damage to premises/property. • Loss – £1K to £10K. • Minor loss of non-personal information.	• Commissioning costs (£) 1m – 2m. • Loss of assets due to minor damage to premises/ property. • Loss – £10K to £100K. • Loss of information. • Impact to service immediately containable, medium financial loss	• Commissioning costs (£) 2m – 5m. • Loss of assets due to moderate damage to premises/ property. • Loss – £100K to £250K. • Loss of or unauthorised access to sensitive / business critical information • Impact on service contained with assistance, high financial loss	• Commissioning costs (£) 5m – 10m. • Loss of assets due to major damage to premises/property. • Loss – £250K to £2m. • Loss of or corruption of sensitive / business critical information. • Loss of ability to provide services, major financial loss	• Commissioning costs (£) > 10m. • Loss of assets due to severe organisation wide damage to property/premises. • Loss – > £2m. • Permanent loss of or corruption of sensitive/business critical information. • Collapse of service, huge financial loss
RESOURCES *(Service and Business interruption, problems with service provision, including staffing (number and competence), premises and equipment)*	• Loss/ interruption < 8 hour resulting in insignificant damage or loss/impact on service. • No impact on public health social care. • Insignificant unmet need. • Minimal disruption to routine activities of staff and organisation.	• Loss/interruption or access to systems denied 8 – 24 hours resulting in minor damage or loss/ impact on service. • Short term impact on public health social care. • Minor unmet need. • Minor impact on staff, service delivery and organisation, rapidly absorbed.	• Loss/ interruption 1-7 days resulting in moderate damage or loss/impact on service. • Moderate impact on public health and social care. • Moderate unmet need. • Moderate impact on staff, service delivery and organisation absorbed with significant level of intervention. • Access to systems denied and incident expected to last more than 1 day.	• Loss/ interruption 8-31 days resulting in major damage or loss/impact on service. • Major impact on public health and social care. • Major unmet need. • Major impact on staff, service delivery and organisation - absorbed with some formal intervention with other organisations.	• Loss/ interruption >31 days resulting in catastrophic damage or loss/impact on service. • Catastrophic impact on public health and social care. • Catastrophic unmet need. • Catastrophic impact on staff, service delivery and organisation - absorbed with significant formal intervention with other organisations.
ENVIRONMENTAL *(Air, Land, Water, Waste management)*	• Nuisance release.	• On site release contained by organisation.	• Moderate on site release contained by organisation. • Moderate off site release contained by organisation.	• Major release affecting minimal off-site area requiring external assistance (fire brigade, radiation, protection service etc).	• Toxic release affecting off-site with detrimental effect requiring outside assistance.

WH&SCT RISK MATRIX – WITH EFFECT FROM 1 OCTOBER 2013

• Risk Likelihood Scoring Table			
• **Likelihood Scoring Descriptors**	• **Score**	**Frequency** (How often might it/does it happen?)	• **Time framed Descriptions of Frequency**
• Almost certain	5	Will undoubtedly happen/recur on a frequent basis	Expected to occur at least daily
• Likely	4	Will probably happen/recur, but it is not a persisting issue/circumstances	Expected to occur at least weekly
• Possible	3	Might happen or recur occasionally	Expected to occur at least monthly
• Unlikely	2	Do not expect it to happen/recur but it may do so	Expected to occur at least annually
• Rare	1	This will probably never happen/recur	Not expected to occur for years

	Impact (Consequence) Levels				
Likelihood Scoring Descriptors	**Insignificant(1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost Certain (5)	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
Likely (4)	**Low**	**Medium**	**Medium**	**High**	**Extreme**
Possible (3)	**Low**	**Low**	**Medium**	**High**	**Extreme**
Unlikely (2)	**Low**	**Low**	**Medium**	**High**	**High**
Rare (1)	**Low**	**Low**	**Medium**	**High**	**High**