

Walton Centre

Incident Response (Operational)

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain	

Table of Contents

Section	Contents
1	Introduction
2	Responsibilities Within This Standard
3	Incident Response – Helpdesk Logging & Resolution
	3.1 Logging
	3.2 Corporate Risk Register
	3.3 Escalation
	3.4 Monitoring & Closure
4	Compliance

1. Introduction

Information and information systems are important assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the Trust .

The Trust acknowledges that we must demonstrate to our stakeholders our commitment to, and delivery of, effective information governance.

The aim of the Trust Governance Policy, Standards and Guidelines is to maintain the quality, confidentiality, and availability of information stored, processed and communicated by and within the Trust. These policies, standards, guidelines are used as part of the information security management system (ISMS) within the Trust.

The Trust places great reliance upon the robust application of the policies and standards that make up the ISMS and has, therefore, developed processes to self assess compliance and for independent review, by its internal auditors.

This standard applies to all staff, whether permanent, part-time or temporary with responsibilities defined below.

2. Responsibilities Within This Standard

All employees using IT equipment, the internet or e-mail have responsibilities with regard to this standard. Particular responsibilities within the standard are defined as:-

Review and Maintenance	Information Security Officer
Approval	Information Security and Governance Group
Local adoption	Line managers (in scope)
Compliance	All staff and contractors (in scope)
Monitoring	Information Security Officer Information Security Auditor

3. Incident Response – Helpdesk Logging & Resolution

3.1 Logging

Incidents that are defined as operational will be reported to and recorded by the helpdesk.

The help desk is manned from **Insert detail** Monday to Friday with an out-of-hours/emergency provision (at senior manager level) that can be contacted through the main switchboard. The desk is manned on a daily rota between the two engineers and the senior engineer. Calls that require a personal visit are assigned to a member of the team currently manning the engineer's desk, with the remaining support person providing back-up and progressing any planned work (installations, system builds etc.)

Upon calling the help desk (**Insert detail**), the person manning the phone will identify himself to the caller and will ask for the following information regarding your call:-

- Name of caller:
- Name of person requiring assistance (if not the above):
- Contact Telephone/Bleep Number(s):
- Nature of problem:
- Equipment identification details where necessary:
- Realistic assessment of the call priority:

In return, the help desk operator will log the call onto the call management system and an e-mail will be automatically generated and sent to the support team and copied to the user, and confirmed verbally where requested. The e-mail will confirm the details as recorded above including priority of the call – which when cross referenced with table 1.1 will give the user an indication of the expected fix time.

All call will be given a call reference and will be assigned a priority on the following basis:-

Table 1.0

Call Priority	Definition
Low	System glitch where there is a work-round available / Enhancement request / Purchasing Requests.
Medium	Prevents user from performing a minor function for which they are employed.
High	Prevents user from performing a core function for which they are employed.
Urgent	Where the issue has a direct impact on clinical care
Immediate	Where the issue has a direct impact on clinical care / Task is time-dependent (i.e. a missed deadline negates the request)

3.2 Corporate risk register

It is intended that Information Security incidents should feed corporate incident reporting. Where appropriate, incidents will also be recorded in the corporate risk management system (which is outside of the scope of this ISMS)

3.3 Escalation

Table 1.1 details the resolution and escalation time-scales (in business hours) attached to support calls based on their assigned priority. Table 1.2 details the staff member charged with managing an escalated call at the appropriate stage. When a call is re-assigned through the escalation process an email notification is automatically sent to the line manager.

Table 1.1

Call Priority	Target Fix	Escalation Level 1	Escalation Level 2	Escalation Level 3	Escalation Level 4
Low					
Medium					
High					
Urgent					
Immediate					

Table 1.2

Escalation Level	Assignee	Tel	Email
1			
2			
3			
4			

3.4 Monitoring and Closure

Outstanding jobs will be subject to on-going monitoring. This process requires a weekly review of all outstanding calls and commentary on the reasons that these have not been resolved.

Upon resolution of the call this will be recorded by the helpdesk.

4. Compliance

4.1 Responsibility

It is the responsibility of all users to ensure that they have read, understood and abide by this standard.

4.2 Review and Monitoring

The Trust has in place routines to regularly audit compliance with this and other standards.