

Document No. ISMS/EPA/01	IT Operations Enforced Path Policy	=
-----------------------------	---	---

1. Approval and Authorisation

Completion of the following signature blocks signifies the review and approval of this Process (signed copy held in safe)

Name	Job Title	Signature	Date
Authored by:- <Name>	Technical Support Officer		
Approved by:- <Name>	Information Security Officer		
Authorised by:- <NAME>	Director of Finance & IT		

2. Change History

Version	Date	Reason
Draft 1.0		First draft for comments
Version 1.0		First Version

Document No. ISMS/EPA/01	IT Operations Enforced Path Policy	=
-----------------------------	---	---

3. Contents

1. Approval and Authorisation.....	2
2. Change History	2
3. Contents	3
4. Definition of Enforced Path.....	3
5. Introduction	3
6. Enforced Path Structure and Mechanism.....	3

4. Definition of Enforced Path

An “enforced path” takes a user from their workstation to the service(s) that they are authorised to use with out risk of accessing, either by mistake or design, other services which they are not authorised to use. This thus stops accidental damage to information or applications. The “enforced path” reflects the privileges set up for the user during their service registration and restricts an application’s access to a specific range of workstations.

5. Introduction

The Trust has several information systems held on various computer systems. Many of these information systems are essential to the operations and business of the Trust. Business and other confidential information is held on these systems thus it is necessary to protect these systems from access by unauthorised users who might also cause damage, accidental or otherwise, to the information held in those systems.

All of the Trust’s computer-based information systems are accessed via the XXXXX () system. It is through XXXXX that access to all the Trust’s computer-based information systems is controlled. Each user has an account and password on the XXXXX system. Each user’s account gives him or her access to certain applications/information systems – this is dependent on which application user groups the user is assigned to.

The majority of users of the Trust’s computer-based information systems are “in-house” users. That is, they use XXXXX at one of the Trust’s sites at Site 1, Site 2, Site 3 or Site 4. The rest of the Trust’s users access XXXXX via dial-in networking from remote sites (such as their homes or via lap-top pc from other remote sites). In both of these cases “Enforced Path” methodology is used to get users to the applications they need.

6. Enforced Path Structure and Mechanism

The enforced path that is employed by the Trust is designed to ensure that end-users only have access to those application and data areas for which they are authorised. The restrictions are controlled by the IT Operations Manager and the Desktop Business Systems Development Manager and are implemented by the IT Operations Department.

There are two methods which constitute, between them, the Trust's enforced path, these are:

1 use of thin-client work-station technology (either pcs or terminals) only allows services to be delivered by XXXXX. Users have no option available but to access XXXXX since settings within the work-stations and the network do not allow other systems to be accessed.

2 the user logs into XXXXX using a unique username (& password!) and once he or she is in the system XXXXX controls what they can do by use of user groups. The user groups allow access to a certain system (or systems) only.

The proxy server controls access to the Internet and individual systems such as the <sewrver type> have their own user account/username/password systems that allow users into permitted areas of those systems.