Walton Centre

Access and Authentication (network)

Document History

Date	Version	Author	Changes
01/10/04	1.0	A Cobain L Wyatt	
31/03/05	1.1	L Wyatt	Update to procedure

Table of Contents

1. Introduction

Information and information systems are important corporate 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 the public, third parties and other stakeholders our expertise in security technology and implementing it. To achieve this it is recognised that we must protect our own assets as well as the environment.

The aim of the Trust Security Policy, Security Standards, Policies & Procedures library is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the Trust. These standards, procedures and policies are used as part of the information security management system (ISMS) within the Trust.

The Trust has implemented several countermeasures and checks to ensure integrity and confidentiality of its information and network devices. These Standards and Procedures outline the way in which we prevent unauthorised access to our network assets.

This document will include the following sections:

- Authentication
- Access to Management consoles
- User and access rights

2. Responsibilities Within 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. User Registration, Changes and Deregistration

3.1 Registration

All users shall be subject to a formal user registration and deregistration process.

This process will require liaison with the Trust Human Resources function and with line managers.

In order to access Trust systems users will be required to:-

- Be sponsored by an individual within the Trust (generally their line manager), this will take the form of a new user form
- Attend a face to face meeting with the registering officer
- Provide “real world” and “active in the community” credentials to verify their personal details, including the home address, copies of which will be retained by the Human Resources Department. These must be current documents and, in the case of “active in the community documents” must not be more than three months old.
- have a clearly defined role based access profile.

This process is in accord with the processes established for the deployment of registration authorities for access to national applications.

See appendix

3.2 Changes

All changes to user access should be requested by a designated “sponsor” (see above). Requests must be in the form of a completed Access Profile Change Request Form.

3.3 Deregistration

It is the responsibility of line managers to advise the IT Department of leavers prior to the termination of employment, clearly recording the last working day.

The IT Department will disable accounts on the date defined above.

The Human Resources Department are required to provide a monthly summary of leavers to the IT Department in order that IT may confirm that all accounts have been locked. Where IT have not previous actioned the disabling of the account due to the absence of information from the relevant department the account will be immediately disabled and the line manager advised of the fact and of their responsibility to advise IT in a timely manner.

Where an employee has been dismissed as a result of disciplinary action the IT Department must be notified immediately by Human Resources in order that the user account can be immediately disabled.

To support this process, accounts will be automatically disabled after x days of inactivity. If a user requires the account to be reactivated they must verify their credentials to the network manager.

4. User id's

4.1 Allocation of id's

All Trust IT staff will be given an individual user access account and logon credentials, to allow access to the Trust network,.

Where possible the "administrator" user id will be changed to a less obvious id. This id will be stored in a sealed envelope with any associated administrator passwords (see below).

All "guest" accounts will be disabled.

Under no circumstances must any unauthorised personnel have access to the Trust's network.

4.2 Segregation of Duties

It is important, in ensuring accountability within the security of the network, that network management and operational activities are clearly separated. To this end:-

- Administrator id's will be allowed for use were required (i.e. cluster admin) or needed as proof to a third party when resolving an issue.
- Users who are responsible for network or system management will be allocated an individual system admin account with appropriate privileges. This account will be used solely by that individual and only for the purposes of system administration. This account will not be used for "business activities"
- Where staff above have a requirement for operational access to systems separate user id's will be issued with access privileges granted on the basis of access required.

This process, as well as representing good management practice, is in accord with the principle of role based access which is being introduced within national programme for IT solutions.

5. Password management

5.1 Administrator passwords

The password associated with administrator accounts on the network or network devices will be changed from the default settings to a random alpha-numeric string consisting of at least x characters.

These passwords will be stored in a sealed envelope with the relevant user id in the fire safe.

5.2 User passwords

Network user passwords will be set in accordance with the security options defined within section 6.

6. Windows Security Options

The Windows operating system allows many security related options to be configured for the network. Defined below is the configuration to be applied to these security options.

6.1 Domain Policy

POLICY	SETTING
Password Policy	
▪ Enforce password history	
▪ Maximum password age	
▪ Minimum password age	
▪ Minimum password length	
▪ Passwords must meet complexity requirements	
▪ Store passwords using reversible encryption	
Account Lockout Policy	
▪ Account lockout duration	
▪ Account lockout threshold	
▪ Reset account lockout counter after	

6.2 Server Policy

AUDIT POLICY	SETTING
Password Policy	
Audit account logon events	
Audit account management	

AUDIT POLICY	SETTING
Audit directory service access	
Audit logon events	
Audit object access	
Audit policy change	
Audit privilege use	
Audit process tracking	
Audit system events	
Restrict guest access to the application log	
Restrict guest access to the security log	
Restrict guest access to the system log	
Retention method for the application log	
Retention method for the security log	
Retention method for the system log	
Shut down the computer when the security log is full	
Security Options Policy	
Additional restrictions for anonymous connections	
Allow servers operators to schedule tasks (domain controllers only)	
Allow system to be shut down without having to log on	
Allowed eject to removable NTFS media	
Amount of idle time before disconnecting session	
Audit the access of global system objects	
Audit use of back-up and restore privilege	
Automatically log off users when logon time expires	
Automatically log off users when logon time expires (local)	
Clear virtual memory page file when system shuts down	
Digitally sign client communication (always)	
Digitally sign client communication (when possible)	
Digitally sign server communication (always)	
Digitally sign server communication (when possible)	

AUDIT POLICY	SETTING
Disable CTRL+ALT+DEL requirement for logon	
Do not display last user name in logon screen	
LAN Manger Authentication Level	
Message text for users attempting to log on	
Message title for users attempting to log on	
Number of previous logons to cache	
Prevent system maintenance of computer account password	
Prevent users from installing print drivers	
Prompt users to change password before expiration	
Recovery console: Allow automatic administrative logon	
Recovery console: Allow floppy copy and access to drives and folders	
Rename administrator account	
Rename guest account	
Restrict CD-ROM drive access to locally logged on user only	
Restrict floppy drive access to locally logged on user only	
Secure channel: Digitally encrypt secure channel data (always)	
Secure channel: Digitally encrypt secure channel data (when possible)	
Secure channel: Digitally sign secure channel data (when possible)	
Secure channel: Require strong session key	
Send unencrypted password to connect to third party SMB servers	
Shut down system immediately if unable to log security events	
Smart card removal behaviour	
Strenghten default permissions of global system objects	
Unsigned driver installation behaviour	
Unsigned non-driver installation behaviour	
File Access Control Lists Policy	

AUDIT POLICY	SETTING
%systemdrive%\	
%SystemRoot%\Repair %SystemRoot%\Security %SystemRoot%\Temp %SystemRoot%\system32\Config %SystemRoot%\system32\Logfiles	
%systemdrive%\Inetpub	
Services Policy – all services not listed should be disabled if not required	
COM+ Event Services	
DHCP Client	
Distributed Link Tracking Client	
DNS Client	
Event Log	
Local Disk Manager to date	
Local Disk Manager Administrative Service	
Netlogon	
Network Connections	
Performance Logs & Alerts	
Plug & Play	
Protected Storage	
Remote Procedure Call	
Remote Registry Service	
Security Accounts Manager	
Server	
System Event Notification	
TCP/IP NetBios Helper Service	
Windows Management Instrumentation Driver	
Windows Time	
Workstation	

7. Compliance

7.1 Responsibility

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

7.2 Review and Monitoring

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

Appendix A

Registration Policy and Practices for Level 3 Authentications

Insert detail