PURPOSE

This Information Security Standards document is the required standard for controlling access to electronic information resources within the HBDHB network.

Access Controls exist to:

- Ensure that only authorised individuals gain access to information assets and that individual accountability is assured wherever possible
- Minimise risk to information assets yet allow business activities to proceed unhindered
- Provide authorised users with access privileges which are sufficient to enable them to perform their duties but do not permit them to exceed their authority
- Prevent inconvenience, critical loss, corruption of data or fraud

PRINCIPLES

The access control standard mandates that:

- All access to information resources is forbidden unless expressly permitted
- Access is granted on the least privilege principle, i.e. only the minimum privileges necessary to complete a business function will be granted
- Job functions and roles are defined that specify the required information processing systems, privileges and associated information for individuals holding that role or function
- Functions, roles and access controls are consistent across the organisation and customers
- Access controlled by legislation is compliant with such legislation

SCOPE

Access controls and business requirements

In HBDHB access controls must be applied to assets to ensure information is protected and to certify confidentiality, integrity and availability. Access controls must comply with this standard to ensure consistency throughout the organisation.

User and group access rights must be configured according to business requirements and the "Least Privilege" principle, see User Access Management in section 2.4.

Documented procedures must control how access is granted to information systems, services or how such access is changed so as to prevent unauthorised access to data or system resources.

A usage profile, detailing privileges and access rights must be assigned to every user. Special attention must be given to access rights that can override system controls.

When access for a user is approved, an administrator must observe this standard and related procedures when provisioning system accounts.

Administration accounts must be strictly controlled and subject to special authorisation by the HBDHB Leadership Team.

The Service Desk logging tool must be used as the central register of identities, defining every HBDHB-authorised user and every system that the user has access to. This is to ensure that a user departure from the organisation has a reference point to identify all systems accessed by that user. The Service Desk logging tool must be the central register because some access to systems such as ECA do not require an Active Directory account. In addition, the system will maintain a complete and up-to-date list of all users having access to each system.

Active Directory must control authentication to systems and applications unless authorisation is granted to use an alternative approved control system.

Immediate termination of access for any system user, including the System Administrator and OS-level managers must be centrally controlled, require collusion and suitable authorisation.
Bespoke applications developed for HBDHB prior to the acceptance of this standard may seek an exception from specific clauses of this standard. However when the risk is assessed as being higher than the cost of retrofitting controls to this standard, then controls must be implemented.

Authentication

Systems with access controls in place must incorporate an authentication phase. The authentication phase will consist of single factor controls or better.

Identification credentials that are presented for authentication may be of the following types:

- Type 1 – Something the entity knows such as username and password or PIN.
- Type 2 - Something the entity has such as a token or smartcard.
- Type 3 – Something the entity is, such as a fingerprint or retinal print or any agreed DHB sanctioned authentication capability.

The majority of HBDHB authentication credentials are one factor and are comprised of a unique username and password. These must be issued to staff when system access has been granted.

Where usernames and passwords are used the following must be observed for single factor authentication only:

- Passwords must be kept confidential and not shared with anyone
- Passwords must not be written down
- Non-System Passwords must be changed every sixty (60) days
- Passwords must not be transmitted, stored or communicated in clear text
- Complex Passwords must be used for all System accounts
- Logs must be maintained for any failed attempts to systems accounts and is raised via an alert
- Passwords must be a minimum of 8 characters
- Passwords must not contain proper names or full dictionary words
- Password caching must not be used

Passwords must be made up of a combination of the following:
- Upper case characters (A-Z)
- Lower Case Characters (a-z)
- Digits (0-9)
- Special Characters (?>:})

It is recognised that clinical applications that are only accessible once a user has authenticated to an operating system may be exposed to reduced risk of unauthorised access. Therefore, it is permitted to consider longer password lifetimes for standard user accounts in these types of

applications. Clinical risk and usability factors should be carefully considered when selecting password lifetimes.

Multiple successive failed authentication attempts must disable the account until it is reset by an authorised administrator. The number of failed attempts must be a minimum of three and a maximum of ten depending on the network location and the classification of data within the system. The standard recommends that the higher the classification of the data or the closer to the network boundary the system is, the lower the attempts permitted.

Accounts that show no activity for longer than three successive calendar months should be disabled.

Systems must enforce a password history control which restricts users from continuing to use the same password after password expiry. The password history control must record at least eight previous passwords.

Systems must enforce a minimum password age control which restricts users from changing a password multiple times in order to bypass the password history control. The minimum password age should be at least 24 hours. This control may be overridden by an authorised administrator when a reset is required.

Password databases must be audited at set intervals to ensure weak passwords are not used.

This task may only be performed by an authorised auditor.

Where digital certificates are used for authentication the following must be observed:

- The certificate must be supplemented with a password for its use at initial issue
- The root certificate used to sign all trusted keys must not be stored in software
- The certificate must have an expiry no longer than one year
- The certificate authentication system must check a valid Certificate

Revocation List (CRL) on presentation of credentials.

- Revoked certificates must be automatically placed on the CRL
- Private keys must not be transported outside of HBDHB premises or in clear text
- Suspected loss or compromise of certificate information should be immediately reported

Where Smartcards are used for authentication the following must be observed:

- The card should be handled, stored and treated as one would handle a credit or bank card.
- Loss of a Smartcard should be reported immediately and its access revoked.
- Smartcards must only be used in approved Smartcard readers within

HBDHB or customer premises

- Smartcard stocks must be kept in a secure zone[1]
- Smartcards must not be shared, borrowed or loaned
- The Smartcard PIN number must be kept confidential and should be unique
- Smartcards are the property of HBDHB and are therefore to be returned on demand

[1] See Physical Security Standard

AUTHORISATION

HBDHB must forbid access to all computing and network resources until authorisation is expressly permitted and granted.

Authorisation is granted via the 'Request for Computer Access Form'. This form once completed must be authorised by the hiring manager and system or information owner. The HBDHB service desk maintains the user authorisation and provisioning procedure.

Access will only be granted once proper authorisation has been received.

System owners or managers must initially sign off access control requests.

All information processing systems must display a notice prior to authentication that access to the system is granted to authorised users only and that unauthorised access is prohibited.

Access controls for highly sensitive information or high risk systems are to be set in accordance with the value and classification of the information assets being protected. Further information can be found in the document

'Asset Classification Standard'.

User Access Management

Users will be granted access to applications by role. This will be an automatic process on entry to the role and will be approved by the staff manager.

Workflow must exist to ensure that the process of employee entry and exit and thus access control registration is approved before access is granted.

All staff will be required to read and understand the responsibilities described in the document 'IS Security Access Policy' and to sign the 'Internet Acceptable Use Form' before access to HBDHB is granted.

Privileges will be assigned to users based on a job role and the minimum privileges necessary to complete that role will be applied i.e. the principle of least privilege will apply.

All staff are responsible for the security of their individual passwords. User password responsibilities are outlined in this document and password standards are defined in section 2.2 Authentication.

All information systems will require an individual password for access.

Shared or group passwords will not be used for critical systems. Exceptions to this are **READ ONLY** accounts provisioned to allow anonymous access to HBDHB resources, i.e. web based databases.

Special privileges that are granted outside of a staff members' job role must be approved by their manager. These special privileges must be reviewed on a quarterly basis.

Information classified as public and published to Internet facing web servers will grant anonymous **READ ONLY** access to read the information.

Information that provides a revenue stream to HBDHB or is otherwise classified as **CONFIDENTIAL or RESTRICTED** and is published to Internet facing applications will be restricted to authorised users only.

External authorised users must read, understand and accept an agreement describing the terms and conditions of system use.

External authorised users accessing commerce systems where write access is granted to an authoritative information system will be required to use a two factor authentication system to grant and control access and allow for non repudiation of transactions. See section 2.2 Authentication.

Where digital certificates are used to authenticate external users, the external user must be responsible for the security of the personal private key

NETWORK ACCESS CONTROL

HBDHB will operate a fully switched network for all data and voice traffic.

Hubs are only permitted for network analysis or in test facilities or during emergency situations until a switch becomes available.

HBDHB will operate the TCP/IP protocol suite across all Local Area Networks (LAN). Only protocols designed to work within this suite may be used on the LAN.

All LAN users will have full unrestricted access to any port or service offered by the TCP/IP suite provided they have the necessary privileges to access the port or service.

All network services will be accessed via applications within the HBDHB environment. No user shall manually craft a datagram, frame or packet of data for direct insertion onto the network. Exceptions to this may be approved by the IT Operations Manager for advanced troubleshooting.

No user shall 'sniff' or analyse the network data without express permission to do so from the IS Leadership Team.

Staff are not permitted to operate a modem from a device on the HBDHB enterprise network without prior approval from the S Leadership Team. Modems that allow incoming calls are expressly forbidden.

All staff with access to the Internet will be restricted to a distinct set of protocols provided by proxy services. Desktop clients and applications must use proxy services for outbound access to the Internet. No direct Internet access is permitted. Exceptions to this standard must be approved by the IT Operations Manager and explicit source, destination and service objects be defined in the boundary firewall.

In general, users will be permitted to use HTTP, HTTPS and FTP protocols via proxy services. DNS requests to public networks should not be necessary for general clients. Instant messaging protocols that allow direct access to Internet based IM services are not recommended. Where IM is required external to the organisation, the use of a proxy is encouraged.

Further, specific applications are authorised to use the following protocols for Internet communication. These applications must be either proxied from the secure network or located in a non-trusted segment such as the DMZ[2].

- SMTP on TCP Port 25
- DNS on TCP and UDP port 53

Access to the HBDHB network for external unauthorised users is prohibited.
Authorised users will comply with policy.

External connections to the HBDHB network are permitted only for the purposes of:

- Remote access for employees.
- Third party management, outsourcing or approved vendor access.

All Users accessing the network remotely are specifically responsible for maintaining best security practices to ensure the security of the HBDHB enterprise network.

Remote Access Users are constrained by the details defined in the document 'Remote Access acceptable Use policy'. All staff accessing the network remotely must receive training on their security responsibilities.

Third Party access to the HBDHB enterprise network will be permitted using the following methods only:

- Virtual Private Network – To a VPN device at the network boundary[3]
- Leased private circuit – To a routing device at the network boundary
- Private Metropolitan Area Network – To a routing/switching device at the network perimeter

All Third party connections to the enterprise network must terminate at the HBDHB perimeter firewall.

Third Parties must sign a "Remote Access Acceptable Use Form" prior to service provision. Third Parties must also prove that a firewall or perimeter defence device is being correctly utilised to prevent hijack of services to HBDHB.

All Third Party access will be monitored and audited for appropriate content and services.

All HBDHB systems providing remote network access will require authentication.

All public Internet accessible services will reside in a de-militarised zone (DMZ)[4].

[2] See Network Zoning Standard
[3] See Network Zoning Standard
[4] See Network Zoning Standard

OPERATING SYSTEM ACCESS CONTROL

The following operating systems are in use within HBDHB:

- Red Hat Linux
- Windows 2000 Server
- Windows 2003 Server
- Windows 2008 Server
- Windows XP Professional
- Windows 2000 Professional

System Administrators will ensure that each operating system will lockout accounts after multiple bad attempts until an administrator unlocks the account. See 'Authentication 2.2'.

System Administrators will ensure that each operating system will generate and log an alert after a bad password attempt or failed authentication.

All operating systems will maintain audit information detailing successful and failed login attempts and failed object access due to insufficient privilege or denied access.

Operating systems will enforce a method to prevent unauthorised access after a given period of idle time that indicates that the workstation has been left unattended. This method will typically be a password protected screensaver that requires authentication by the logged in user or an administrator to remove. This will not apply to a clinical workstation.

The recommended period for screensaver activation is after fifteen minutes of idle time.

All management tools and system utilities must be restricted to administrative use only.

Where appropriate and in conjunction with the segregation of duties concept, administrative duties will be spread between several dedicated systems administrators.

Where appropriate, systems administrators will receive differing levels of privilege and access to system utilities depending on their skill level and experience.

Systems administrators must receive administrative accounts to perform administrative tasks. These must be separate from the accounts used for everyday tasks such as reading mail or writing documents.

The administrative accounts should be used either to logon to management hosts, servers or via the 'run as' command which allows individual applications to be executed in a different context

APPLICATION ACCESS CONTROL

Applications may be accessed either by directly presenting identification credentials or via a transparent pass through (single sign-on) of identification credentials.

Where transparent pass through or single sign-on is used, the credentials may not be passed in clear text across the network. For authentication systems that do not support encryption in the authentication stream, an encryption layer must be used i.e. SSL or IPSEC.

Applications should use the centralised Active Directory for authentication services.

Applications should control authorisation via a centralised authorisation model. The use of code snippets, includes or custom controls on each protected resource should be avoided.

Bespoke applications should use the authorisation and authentication frameworks inherent in the development language. Microsoft NET is the preferred development framework at HBDHB and contains an authorisation model capable of centrally managing authentication within the application.

Session state must be managed by the application to guarantee the integrity of the authorisation status. Session management should not rely on client side components such as cookies, request headers or hidden fields unless appropriately secured using cryptographic methods. Where possible, use the session management capabilities of the development framework and ensure that session details are validated at the server side.

Applications should regularly check authorisation status over the life of a user session from the authoritative source. Idle sessions must be identified and discarded.

The recommended session lifetime for idle timeout or revalidation is between five and fifteen minutes and is dependent on the classification of the information inherent in the application. These values are based on industry recommendations and are not necessarily specific to the health sector. Clinical risk and system usability should be carefully considered when selecting timeout values.
The principle of least privilege must apply to applications and application services. This means that:

- Development test and staging services must also run with least privilege to ensure that production operates correctly with least privilege.
- Accounts that are used to run applications should not have high levels of privilege i.e. Administrator, SA, Local System etc.
- Accounts used for applications should be created as unprivileged accounts and then granted privileges as required. An application account should not be given all privileges and then limited.
- Accounts used by an application to access a database should never have the privileges necessary to modify the database schema. Database access accounts should only be granted the necessary read or write privileges to specific database objects.
- Applications should call database stored procedures and views rather than constructing queries real time. The construction of queries by the application may allow the user to insert unauthorised parameters.
- Administrative and user accounts must be separated even if the user is required to operate across both realms.

ACCOUNTING

Audit trails and event logs must be maintained for each information processing system. As a minimum, these must provide information regarding:

- Logon/Logoff – Time, date, successful, unsuccessful, user ID, # attempts
- Originating workstation – Address or name
- Object Access – Time, date, unsuccessful, user ID

All authentication is to be logged and monitored by automatic auditing within Active Directory or individual application identity stores to identify potential misuse of systems or information.

When defining monitoring for new systems, the threats and vulnerabilities to the system must be assessed to produce a risk profile. This profile will dictate the level of monitoring required.

System logs must be centralised and available for review to the following groups:

- Read access for system administrators for troubleshooting and review
- Full access for system auditors

All system clocks must be synchronised with an enterprise timeserver at logon or as a scripted batch every 24 hours. The enterprise timeserver will synchronise using NTP.

For audit and accountability purposes it is imperative that access to systems is assigned to individuals. Default or generic accounts should not be used for accessing systems and should be removed where possible.

MOBILE COMPUTING AND TELECOMMUTING

All users of mobile computing or telecommuting equipment will be required to have read the standard 'Cellular Phone Policy' as published on HBDHB's intranet "Nettie" before equipment is issued.

All users of mobile computers or Telecommuting facilities are solely responsible for the security of the equipment in their possession.

All staff in possession of mobile computing equipment shall ensure that:

- Virus definitions are current and are kept up to date regularly. This should be automatic
- An appropriate protection technology is in place and correctly configured to protect the device from malicious attack or unauthorised access
- Mobile computing devices are not left unattended
- Mobile computing devices are suitably protected from theft using an appropriate locking mechanism and identification marking

HBDHB files and other information are stored within the corporate network and not stored locally on the mobile device. Work in progress may be stored locally but must be uploaded to the HBDHB enterprise network when next connected and the local copy deleted. RESTRICTED[5] information should not be stored locally.

[5] See Asset Classification Standard13

REVIEW OF ACCESS CONTROLS

Access controls should be reviewed periodically and upgraded in response to new threats, capabilities, business requirements or access violations.

HBDHB will review access controls to all systems annually and critical systems quarterly

KEYWORDS

Access
Confidential
Control Standard
Restricted Information
Security
IT

For further information please contact Information Services.

Appendix

Glossary

Term	Definition
Information	Data, required for the operation of an organisation, which is captured, received, generated, processed, stored, manipulated, communicated transmitted.
Classification	The labelling of information in order to determine how it can be processed, stored, communicated, transmitted and accessed.
Staff	Those who have an employment contract with HBDHB and are responsible for HBDHB information in the course of their duties.
Manager	Refers to all staff that have a responsibility for managing employment relationships with other HBDHB staff.
Team Leader	Staff who have a responsibility for managing and leading the business as usual activities of other staff.
System Owners	Those staff responsible for the ownership of information processing systems.
Access Control	Enforces a user's privileges or access rights to an information asset.
Alert	An audited event that is deemed to potentially have a security impact. An assessment will need to be performed on an alert before it can be classified as an incident.
Attack	An attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing counter measures.
Authenticate	To establish the validity of a claimed user or object.
Authentication	To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
Authorisation	The process of verifying an authenticated user has access to requested information resources.
Authorising Manager	A Manager that has the power or privilege to grant permission or is accountable for a particular group, department or cost centre.
Availability	The fundamental requirement to ensure that information is available as and when it is required and protected from unauthorised destruction.
Business disruption	Direct or indirect interruption to normal business practices resulting from compromise of confidentiality, integrity or availability of an information asset.
Breach	A violation of information security policy or standard.
Critical	An indispensable, essential element of the business, without which part or its entire core, HBDHB business objective could not be achieved.
Confidentiality	The fundamental requirement to protect information assets from unauthorised disclosure.
Denial of service	A specific threat where users of information assets are prevented from accessing those assets due to the loss of service availability either via intentional or accidental action.
DMZ	Refers to a demilitarised zone. A military word used within information technology to describe an area of the network usually between un-trusted and trusted resources.
Event	Any observable occurrence in a systems network or physical environment. e.g. System crash, system reboot, earthquake
Firewall	A system or combination of systems that enforces a control boundary between two or more networks. Also known as a Gateway that limits access between networks in accordance with local security policy.
Gateway	A gateway is a point within a network where traffic may enter or leave for another network.

Term	Definition
HIDS	Refers to Host Based Intrusion Detection System. A toolset resident on a host system designed to inspect system access and detect malicious attempts to subvert security policy.
Incident	An adverse event in an information system and/or network that poses any risk to HBDHB, including financial reputation, technological or business risk.
Integrity	The fundamental requirement to ensure that information assets are not subject to unauthorised alteration.
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Malware	Hardware, software, or firmware that is intentionally included or injected into a system for an unauthorised purpose.
NIDS	Refers to Network Intrusion Detection System. A toolset designed to inspect network traffic for suspicious events.
Packet	A unit size of data transmitted across an Ethernet network.
SAML	Refers to Security Assertion Markup Language. This is an XML-based framework for exchanging security information.
Threat	Any circumstance or event with the potential to cause harm to HBDHB information in the form of destruction, disclosure, modification of data, and/or denial service.
Violation	Any action contrary to Security Policy or Standards.
Vulnerability	A weakness in a system or process that may be exploited and allow a threat to occur.