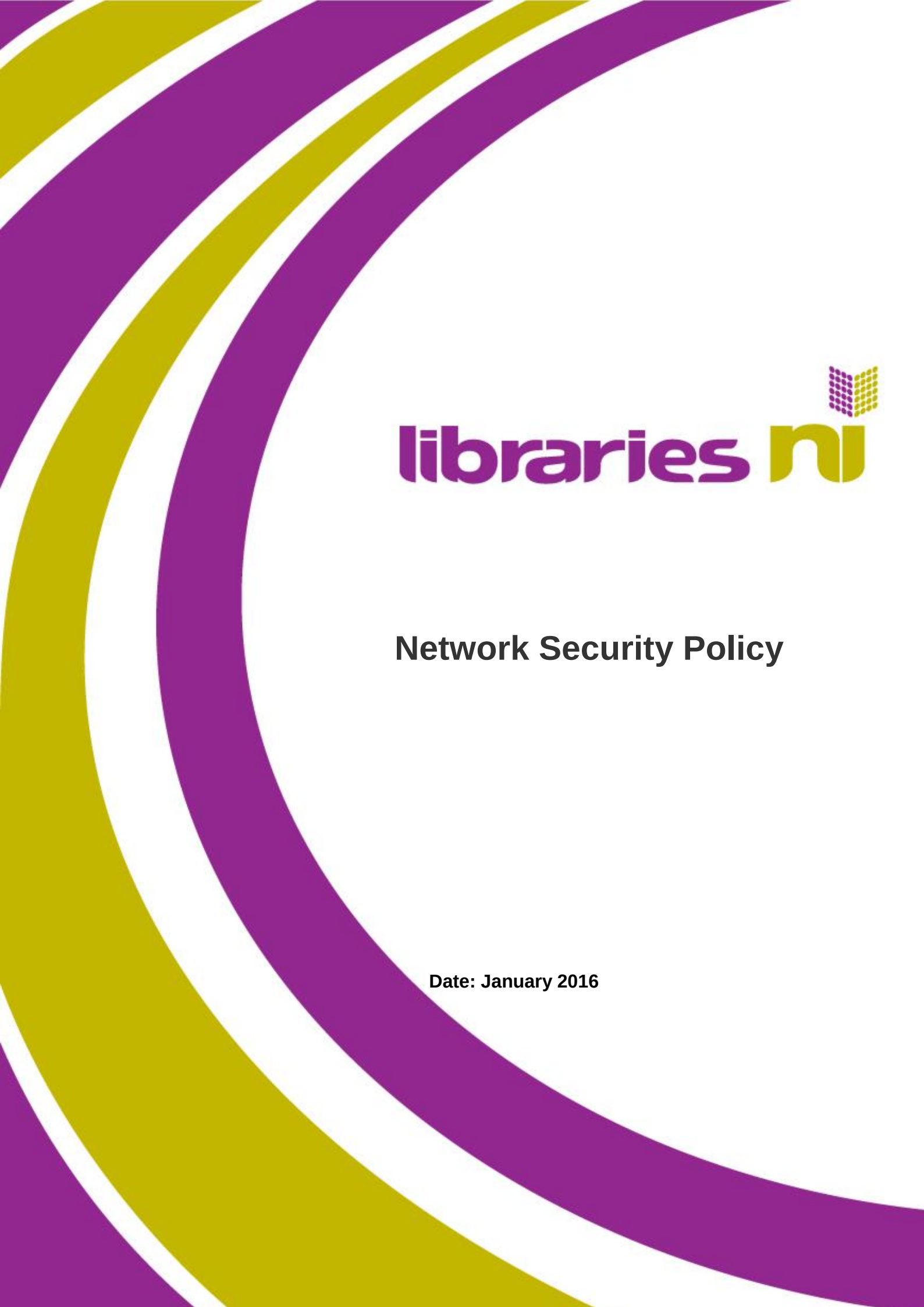

Network Security Policy

Date: January 2016

Policy Title	Network Security Policy
Policy Number:	POL 030
Version	3.0
Policy Sponsor	Director of Business Support
Policy Owner	Head of ICU / ICT
Committee	Business Support Committee.
Date Approved	
Date Screening Documentation Signed	
Date Set For Review	December 2018
Related Policies	POL029 Server Security Policy POL031 Internet Security Policy POL032 Information Security Policy POL033 Microsoft Windows Client Security Policy POL034 Application Security Policy POL035 LNI Staff Acceptable Use Policy

Document Control

Version	Status	Revision Date	Summary of Changes	Author
0.1	*Draft*	21/12/2013	Initial copy from customer	
0.2	*Draft*	04/06/2013	Updated to reflect new service and contract being delivered by Fujitsu	Inderjit Birak
0.3	*Draft*	25/06/2013	Updated following review by Solution Owner	Inderjit Birak
1.0	*Final*	10/09/2013	Programme Board Approval	e2 Project Team
2.0	*Final*	19/09/2013	Information Systems Committee Approval	e2 Project Team
2.1	*Draft*	16/01/2014	Updated to LNI e2 standards	Jamie Aiken
2.2	*Draft*	05/12/2015	Minor changes suggested by SMT	Jamie Aiken
3.0	*Final*	01/2016	Approved by BSC	Jamie Aiken

1. Introduction

This document forms part of the suite of Security Policy documents for Libraries NI.

The Libraries NI environment provides IT services to all Library locations in Northern Ireland.

The Authority will take appropriate steps to protect the IT environment from threats, including but not limited to unauthorised access, computer viruses, violation of privacy and interruption to service.

2. Purpose

This document lays down the minimum security standard applicable to components that form the Wide Area and Local Area Networks within the Libraries NI IT environment. All systems are considered to be at high-risk, but some particularly high-risk systems will need to take additional security steps beyond those prescribed in this document.

3. Policy

3.1 Network backbone

The IT environment consists of a private network that interconnects a Data Centre with library sites and supports both Libraries NI and Public traffic. This network must ensure logical separation of the Libraries NI and Public network traffic. The Libraries NI network is critical to the day to day delivery of library services in Northern Ireland, as it is used for administrative purposes, and for delivery of library management services, and similar functions.

The data network will be an IP-based network. No wide area traffic other than IP protocols will be routed between sites.

3.2 Network design

Wherever appropriate, the Libraries NI network should be separated into different zones, based on the sensitivity of the information being communicated and as a minimum deliver separation between the Libraries NI and the Public network.

Wherever possible, the Libraries NI network should be designed to avoid single points of failure, and to provide at least 99.0% availability.

Control statement: there will be separation between development, test and operational facilities and environments, to reduce the risk of unauthorised access or changes. The environments must be segregated by implementing the most appropriate controls which include but are not limited to:

- Running on separate computers, domains, instances and networks, using for example MPLS, VPN and encryption to ensure the protection of data passing over networks.
- Different usernames and passwords to ensure that changes cannot be made accidentally or intentionally from one environment to the next
- Segregation of duties of staff who have authorised access to the environments and who test operational systems to be achieved whenever appropriate.

Network designs and architecture must be documented and maintained, and to include configuration settings for network hardware and software details.
All hosts must be security hardened using best practice standards to an appropriate level. Operating systems network services are to be reviewed, and those services that are not required will be disabled.

3.3 Wide area network

Essential network services should be placed at sites of greater resilience within the Libraries NI network. Wherever possible, these services will themselves be configured with redundancy spread across a number of sites.

Within the wide area network, dynamic routing protocols (e.g. OSPF) may be used. Unauthenticated dynamic routing protocols (e.g. RIP) should not be used.

Control Statement: Wide area connections within the Libraries NI network must be covered by a Service Level Agreement with the supplier. This SLA must cover the different level confidentiality of Libraries NI and Public data on the network, the interfaces between the supplier and Libraries NI, and the expected availability and bandwidth

3.4 Local area network

LAN cabling and services generally have to be physically accessible within a network. The following security requirements apply to Libraries NI LANs.

Control Statement: LAN cabling provided in public areas should use equipment that restricts the network cards that can be connected to it by implementing as a minimum MAC address filtering on a switch

Control Statement: Newly installed unshielded twisted pair (UTP) cabling must at least be compliant with Category 5e

.

Cabling infrastructure within a building should be anchored into cable trays. Data cables should not be placed in the same cable tray as power cables.

Control Statement: Local area networks must be configured to provide a single router (gateway of last resort, or default gateway) to the rest of the network

Wherever possible, different LANs should be provided for client and server machines, in order to limit the opportunity for unauthorised access to servers. This separation may be provided by VLAN technology. In addition, LANs for Libraries NI and Public client machines should also be separated.

Control Statement: The number of stations within a collision domain must be limited so that network performance is not impaired by collisions

LAN equipment (e.g., hubs, switches) should have unused ports disabled. Cabling between LAN access points and equipment should be labelled and documented to facilitate tracing and troubleshooting.

Control Statement: All LAN access points must be clearly labelled. Documentation and labelling must together facilitate tracing from LAN access points to the network equipment port

Wireless LANs (WLANs) are allowable within Library locations but there must be separate Libraries NI and Public WLANs. Specific technical steps must be taken to ensure this separation including use of different SSIDs.

Control Statement: Wireless LANs must only be attached to the library environment with the explicit approval of the Information Security Manager

3.5 External connections

The connections between the library private network and other networks should usually only occur at the Data Centre.

Control Statement: Connections between the Libraries NI private network and any other network must be protected by a firewall

Firewalls represent the mainline defence for protecting Libraries NI networks and systems from external threats, therefore it is essential that the firewalls are set up and managed appropriately. Access to firewalls and firewall rule sets is to be limited to authorised staff only and all changes subject to strict change control procedures and authorisation before changes are made, to reduce the risk of compromise from internal threats.

Control Statement: Connections between the Libraries NI network and public networks (for example, the Internet) must be protected a firewalls

Control Statement: All connections to the inside of external connection firewalls must terminate on a switch port, or on a LAN that is dedicated to that connection

Control Statement: The security policies applied by external connection firewalls must comply with a default deny posture with communication only permitted if specifically authorised

3.6 Equipment security

Information processing equipment, and cabling carrying data or supporting information services, shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access. Equipment must be physically located in secure areas, protected by appropriate entry controls as necessary.

Equipment shall be correctly maintained to enable its continued availability and integrity and faults and corrective actions recorded in accordance with service management processes for Availability, Event and Incident Management.

Information shall be erased from equipment prior to disposal or re-use. Established processes will be followed to ensure that no piece of equipment or device, which contains data, is removed for disposal unless it is going directly and securely to an approved destruction organisation for disposal.

All equipment and cabling must be maintained and protected against environmental hazards, including fire and water damage.

Equipment shall be correctly maintained to enable its continued availability and integrity. All equipment shall be maintained in accordance with the manufacturers' instructions by qualified and authorised maintenance personnel. A record is to be kept of all maintenance work carried out.

All faults are to be recorded via a documented Fault Reporting System. This system shall also record the work carried out to fix the fault.

Removal of equipment from sites shall be subject to preapproval and authorisation. Equipment belonging to third party suppliers is not to be removed without approval and authorisation from the third party management. All equipment moves (with the exception of the personal allocation of Laptop PCs, PDAs, mobile phones or other equipment specifically allocated for personal use) are to be registered on the equipment asset register

Control Statement: All network equipment including patching facilities must be installed within a secure room or cabinet. Access to the secure room or cabinet is to be restricted to authorised personnel only

Control Statement: Network equipment in critical parts of the network must be provided with UPS to ensure continuity of network service in the event of a power failure

Control Statement: Manageable network equipment must be configured to permit monitoring over Simple Network Management Protocol (SNMP) v3. Configuration changes over SNMP must be restricted to authorised personnel only

Control Statement: Network equipment must be configured to record an audit trail for unauthorised access and the audit trail must be protected from tampering

Control Statement: Network equipment must display an appropriate warning message before allowing access to management functions

Control Statement: Network equipment must run an approved version of its operating software. IT Operation and the Information Security Manager will provide and maintain a list of approved versions and patches. When a version is removed from the list, or a mandatory patch is added, the necessary updates will be applied within a time period agreed with the Authority

Control Statement: Network equipment must not be configured to load new operating software or configuration data automatically. Any such update must be carried out manually by a suitably authorised administrator

Control Statement: All network equipment should be configured to reference a trusted Time Source Server

All network assets and components must be recorded in an asset inventory and assigned an owner.

3.7 Remote Management

Manageable network equipment should be configured in such a way as to minimise the risk of unauthorised access to the management function.
There must be clear documented responsibilities and procedures for the management of remote equipment and users.

Control Statement: Manageable network equipment must be secured by means of a non-trivial password of at least 8 characters, including both alphabetic and numeric characters. This password must be recorded in a

central place, in a secure manner, available only to those authorised to manage the equipment

Control Statement: Secure protocols such as, SSH, HTTPS, must be used in place of telnet for remote terminal connection to any network equipment that supports it. In such a case, the telnet service must be disabled

Control Statement: Remote management functionality must be configured to permit connection only from a limited range of IP addresses

Physical and logical, including remote, access to diagnostic and configuration ports shall be controlled.

3.8 Network connectivity

3.8.1 Registration

In order to maintain up-to-date information about machines connected to the network, IT will operate a registration system.

Control Statement: All equipment connected to the IT network must be registered with IT Operations before it is connected

Control Statement: All equipment connected to the IT network must be assigned a unique name as part of this registration. The names assigned to network backbone equipment should be chosen to assist the easy identification of the location of the equipment

3.8.2 Address allocation and resolution

Network address allocation within the IT network will be the responsibility of IT Operations. Where equipment requires a fixed address, that address will be assigned by IT Operations. The default configuration for allocating addresses to equipment will be via dynamic addressing (e.g. DHCP).

Control Statement: All network addresses in use on the IT network must be recorded by IT Operations

Control Statement: Dynamic address servers (e.g. DHCP servers) must be implemented only by IT Operations

Address allocations will be maintained in central name services (e.g. DNS), and these will be used to resolve addresses.

All servers running TCP/IP within the IT network will be defined within the Libraries NI domain. Internal DNS servers will hold the internal information about this domain within the Active Directory or equivalent.

Internal DNS servers will also provide a means for the resolution of external fully qualified domain names.

3.9 Virtual Private Networks

The use of virtual private networking (VPN) products is preferred for the communication of particularly sensitive data within the IT network, and is also permitted for inbound connection to the IT network from the Internet.

The Information Security Manager must maintain a list of users who are permitted to use VPN functionality for inbound access to the IT network from the Internet.

3.10 Network operations and Network monitoring

Routine network monitoring should be carried out to ensure that all elements of the network backbone are operational, and to initiate remedial action where an element fails or is not performing optimally.

Control Statement: Elements of the network infrastructure must be monitored, in order to identify elements that have failed or are not performing optimally

Traffic monitoring is permitted within the IT in support of troubleshooting and planning activity, but data must be deleted once it is no longer required for this purpose. Packet capture is also permitted for the purpose of investigating any security incident, whether real or suspected.

Control Statement: When capturing traffic for troubleshooting and monitoring purposes, operations staff must ensure this does not lead to the inappropriate disclosure of sensitive information.

All incidents identified on the network are to be reported and tracked in accordance with incident management procedures, including security incidents.

The Information Security Manager is to be notified of security incidents.

3.11 Configuration management

Changes to the network infrastructure should be carried out in a controlled manner, in order that they do not adversely affect the services of the IT environment.

Control Statement: IT Operations must produce and maintain complete documentation on the IT network, and the equipment that makes up the network infrastructure. This documentation must be sufficient to rebuild any network element in the event of its failure and replacement

Control Statement: All changes to components (cabling, routers, servers, etc.) of the IT network must be made in a manner that is compliant with the IT Change Management standards. Formal and approved change control requests are required prior to the change being implemented, in accordance with Change control procedures

3.12 Network planning

3.12.1 Performance monitoring

IT Operations must carry out routine performance monitoring of the IT network, and propose corrective action where traffic levels cause bottlenecks. Performance monitoring will include at least availability, collision rates and error rates.

Control Statement: Elements of the network infrastructure must be monitored, in order to identify performance issues in the network

3.12.2 Network Access Control

In order to protect network services access to internal and external network services shall be controlled in accordance with this policy. To summarise:

- Appropriate authentication mechanisms for users and equipment;
- Device authentication when connecting to LNI;
- Control of user access to network information systems;
- Appropriate inter-network interfaces such as firewalls are to be in place and managed;
- Shared networks shall have routing controls to ensure that computer connections and information flows do not breach access control policies;
- Controls shall be introduced in networks to segregate groups of information services, users and information systems as appropriate;

- Access to diagnostic ports or other facilities must be securely controlled to ensure they are only available to approved persons at approved times;
- Equipment connecting to LNI networks will be uniquely and securely identified;
- Authentication, whereby a user's claimed identity is verified, is essential before any access is granted to any LNI IT system. Authentication mechanisms are required to ensure that trust relationships can be established between communicating components within, and external to, the LNI services;
- All LNI connections with remote computer systems shall be authenticated. The User or application that initiates a transfer shall be authenticated by both the destination and the source node. Authentication must be successful before any transfer is executed; and
- The path from the user PC or workstation to the services provided shall be controlled.

3.12.3 Network Security Management

The overall security of the management of the network is to be conducted in accordance with this policy, to summarise:

- Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit;
- Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced;
- Only authorised and appropriately trained staff are permitted to manage and make changes to network and network infrastructure devices and firewalls;
- All changes to networks are firewalls are to be subject to pre authorisation and approved change control requests in accordance with the change control procedure;
- Remote access to diagnostic ports shall be securely controlled;
- System privileges and access permissions to perform management functions are to be based on the principle of least privilege and access to be auditable and audit logs retained and monitored;
- Segregation of duties is to be achieve wherever appropriate;

- Appropriate encryption and authentication methods to be used for the transmission of sensitive information/data and for remote access; and
- Third party access to processing facilities poses significant risk and therefore must be appropriately managed;
    - A formal risk assessment shall be conducted to identify risks associated with access to information and information processing facilities by third parties and appropriate controls implemented;
    - A formal contract is to be place before access to information and information processing facilities is provided; and
    - Third party access to be subject to review.

4. Waiver from Policy

Request for a waiver from this Information Policy must be address to the Information Security Manager. The request for a waiver must describe why a waiver is required, justification why the policy cannot be adhered to, and a plan to bring the application or system into compliance in the future. The Information Security Manager will discuss waiver requests with senior management, as appropriate.
Waivers can be granted by the Information Security Manager for a period not exceeding one year, but may be extended annually if the justification still applies.

5. Monitoring and Review

The Information Security Manager is responsible for monitoring and reviewing this policy and will conduct a formal review of the efficiency and effectiveness of its application on an annual basis.

6. Violations

Any violations of this security policy should be brought to the attention of the Information Security Manager, who will work with the appropriate individuals to rectify the problem.