NHSScotland

National ICT Infrastructure Standard

NHS SCOTLAND

Digital Health & Care Scotland

eHealth

Document Control

Document Title	NHSScotland National ICT Infrastructure Standard
Version	1.4
Owner	NHS National Infrastructure Leads Group
Authors	Russell Fleming
Created date	17th October 2018
Compliance	See guidance in section 2
Reviewers and Distribution	Reviewers: National Infrastructure Leads & Health Board Digital Leads Distribution: National Infrastructure Group, National Transition Group, Digital Health Leads, Scottish Government Digital Health & Care Directorate.

Version Control

Date	Version	Author	Changes
17/10/2018	0.1	Russell Fleming	Initial draft
25/10/2018	0.2	Russell Fleming	Incorporated feedback from National Infrastructure Leads meeting 19 Oct 18
19/11/2018	0.3	Russell Fleming	Updated to gain endorsement from National Infrastructure Leads Group
15/01/2019	1.0	Russell Fleming	Final approval from eHealth Leads
27/01/2020	1.1	Russell Fleming	2020 Update
11/01/2021	1.2	Russell Fleming	Rearticulated the Application compatibility 'Web components' section (page 6)
24/06/2021	1.3	Russell Fleming	Collapsed the TOM to be current Standard
20/06/2024	1.4	NIG Standards SLWG	2024 refresh

Contents

1. Overview

This document sets out the specification of the NHSScotland ICT Infrastructure Standard. The specification is based on making the optimal use of National licensing agreements.

This standard describes the hardware and software specifications for infrastructure in NHSScotland. It aims to benefit a number of audiences to ensure they are making informed decisions based on the current, as well as the anticipated, availability of IT infrastructure across the NHSScotland estate.

Adherence to the standard will support Boards in local planning, aid procurements by providing specifications and assist suppliers to provide solutions that can integrate with the NHSScotland infrastructure, therefore, leading to more effective solution delivery.

2. Compliance with the Standard

For NHSScotland Boards:

Boards **must** target compliance with the specification and work towards accordance in a planned and consistent way.

For Suppliers:

The standard provides suppliers with the current specification to which their solutions **must** comply. Suppliers should ensure their solutions can be deployed, function and integrate where required with all the relevant specifications detailed in this document.

Non-compliant Solutions:

If a solution is required for specific business or clinical needs but does not meet the specifications set out in the standard then appropriate consultation should be undertaken with infrastructure teams at a local, regional or national level to consider the implications of the increased support and, both the cost, and risk implications, the non-standard product(s) will introduce.

For National and Regional level non-compliant solutions, a quorum of agreement must be reached before the product can be used. This will be established on achieving a minimum agreement of 75% or more on a one Health Board one vote basis. An exception list will be kept and maintained by the National Infrastructure Leads Group Support Officer and will regularly be reviewed by the National Infrastructure Leads Group. The governance for exceptions is covered in Section 16: Infrastructure Management.

Legislative compliance

Legislative requirements, including the UK General Data Protection Regulation 2018 (GDPR), require all public sector organisations to ensure appropriate technical protections are in place when suppliers process personal data on our behalf.

The Security of Network and Information Systems 2018 (NIS) Regulations require that a Competent Authority is in place to ensure that essential service sectors have robust cyber security.

Scottish Ministers are considered to be the Competent Authority for Health in Scotland, as such they have a regulatory responsibility for oversight and enforcement of the NIS Regulations. All NHS Scotland health boards are considered to be Operators of Essential Services and therefore must comply with the standards set out in the NIS Regulations. Standards cover managing security risk, defending systems against cyber-attack, detecting cyber security events and minimising the impact of cyber security incidents.

The Scottish Government Public Sector Cyber Resilience Framework (CRF)

The Digital Health & Care Division on behalf of the Scottish Health Competent Authority conducts formal assessments and audits of health boards to obtain compliance assurance. These audits are structured in a manner consistent with the Public Sector Cyber Resilience Framework (CRF[1]) which has the advantage of providing a framework for the conduct of the audit that allows us to evaluate the effectiveness of risk management, cyber security controls and governance processes. Ultimately the approach enables the health boards to obtain compliance assurance with the NIS Regulations.

Please note the current version of the CRF is under review. The SG Cyber Resilience Unit have drafted PSCRF v2.0. It is the updated draft PSCRF v2.0 which NIS compliance audits are conducted against.

PSCRF v2 incorporates these standards:

- Cyber Essentials: 2022
- Public Sector Action Plan
- Digital First
- 10 Steps
- UK GDPR Security Outcomes
- NIS-CAF 3.1
- ISO 27002:2022
- BS 3111:2018
- CSA STAR / Cloud Control Matrix (CCM)
- ETSI EN 303 645 V2.1.1 Cyber Security for Consumer Internet of Things: Baseline Requirements

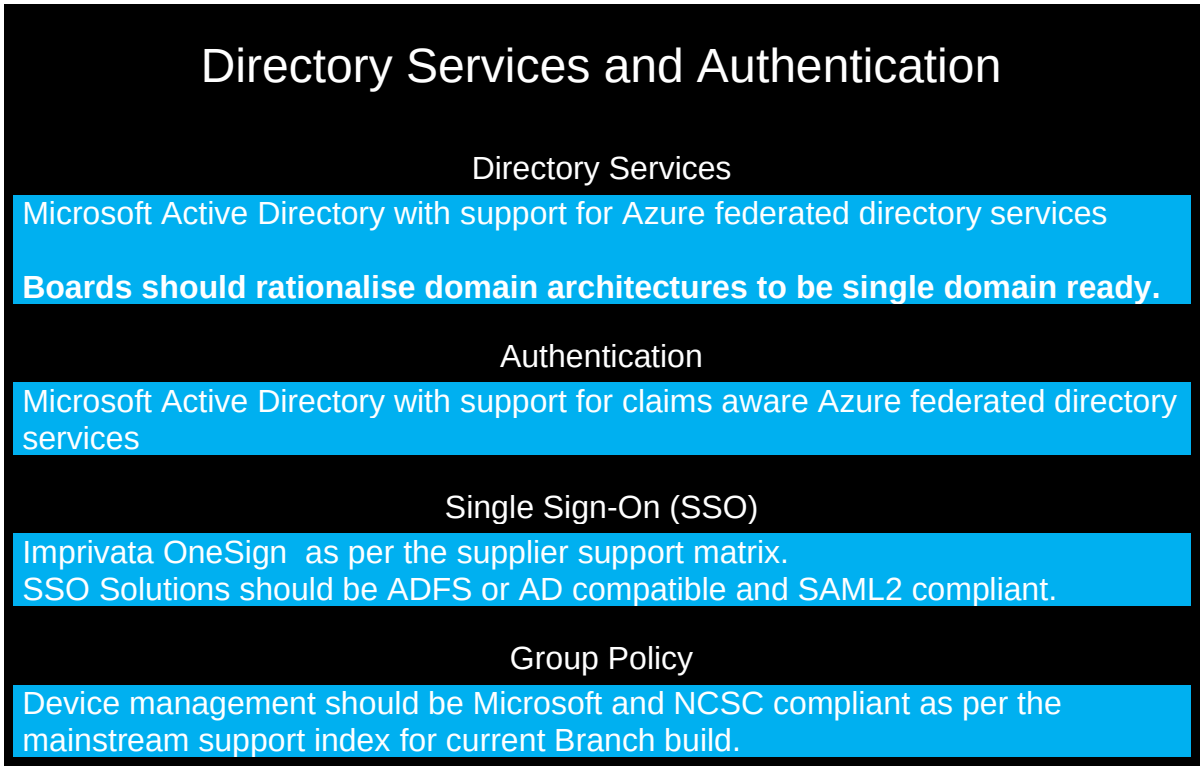
Maintaining supplier support for all systems in use across NHSScotland is a must.

[1] The Scottish Government Public Sector Cyber Resilience Framework (CRF) - Cyber resilience: framework and self assessment tool - gov.scot (www.gov.scot)

3. Document review schedule

This document will be updated on an annual basis, in line with the financial year, to ensure NHSScotland is making best use of National Licence deals and to reflect changes to vendor support road maps. However, there is scope for the document to be reviewed and updated out-with this cycle should the requirement arise. The next scheduled revision of the document should be completed by **31 March 2025**.

4. Directory Services and Authentication Specification



5. Application Compatibility Specification

Recommended specifications for browsers, productivity and core business functionality (excludes line of business and clinical). Methods of application delivery are, in order of preference:

i. compliance with the Web Browser specification.

ii. packaged applications for deployment by Health Board client management tools

iii. delivery of application by desktop virtualisation or thin client technologies

Applications should not require any variation to existing standard builds of the operating system.

Application Compatibility

Application Rights

Installing or running of applications should not require elevated rights for the logged on user. Where there is a legacy application requirement technical mitigation and/or supplementary controls should be used to restrict use to least possible privilege.

Web Browsers

The Nationally Preferred Web Browser for NHSScotland is:

- Microsoft Edge (Chromium) – This should be used as the minimum standard for testing and compatibility for all systems and applications.

Testing and compatibility should also include the other supported Web Browsers:

- Google Chrome (Enterprise Edition Only) - appropriate management must be used to lock down and control the configuration.
- Safari is acceptable on Apple devices only.

All web browser testing should be carried out with NCSC Device Security Guidance[2] and Microsoft Windows Security Baseline[3] recommendations in place

Web Components

- All new systems must use HTML5 compliant solutions for web based applications.
- Legacy systems can continue to use supported versions of Java as per the mainstream support matrix. Open Java is preferred where feasible.
- Applications should not require a fixed version of Java.
- Any supplementary web components need to be maintained in line with current or current –1 support.

Operating System

- All new windows based systems must use Windows 11 (E3 or E5) – Versions must be within a supported Service Branch
- All new Linux based systems must be supported on the latest version as per the mainstream support matrix.

[2] NCSC Device Security Guidance: https://www.ncsc.gov.uk/collection/device-security-guidance
[3] Microsoft Windows Security Baselines: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines

Productivity Tools
• Applications must be able to work with Microsoft Office 365 F3 level licences. • New systems should not require locally installed versions of Office. • PDFs should be set to open in a supported web browser. Adobe Reader should only be deployed on endpoints if absolutely necessary and must be maintained to always provide the latest supported version.
Local Session Data
• Session data created by applications should not be retained on endpoint devices (e.g. local copies of databases). • It is permissible to retain session data on mobile devices in areas where no connectivity is available so long as appropriate encryption is in place.

6. Endpoint Security Specification

Health Board specified solutions, installed and configured in line with NISR and CRF, offering the following:

Endpoint Security
Anti-Virus/Anti-Malware
Required – vendor optional Preferred Solution: Windows Defender Anti-Virus Note: If using an alternate AV solution, Windows Defender must be present on the endpoint, and enrolled into the NHSScotland National Cyber Security Operations Centre (CSOC).
Advanced Threat Protection
Required – vendor optional Preferred Solution: Microsoft Defender ATP
Host Based Firewall
Required – vendor optional Preferred Solution: Windows Defender Firewall

USB port control
Required – vendor optional Preferred Solution: Windows Defender
Disk Encryption
Required – vendor optional – In line with Mobile Data Protection Standards Preferred Solution: BitLocker
Pre-boot Authentication
BitLocker with Trusted Platform Module (TPM)
Screensaver
Screensaver with a screen locking function enabled
Operating System Security
OS Hardening should be implemented as per NCSC End user device (EUD) security guidance[4]
Web/Content Filtering
Required – vendor optional
Local Administrator Password management
MS LAPS
Hard Disk Drive Disposal
Faulty and end of life hard disks are to be shredded or securely wiped using an NCSC certified product and a full audit trail of the process is to be maintained by the local Health Board.[5]

7. Server Security Specification

Health Board specified solutions, installed and configured in line with NISR and CRF, offering the following:

[4] NCSC End Used Device Security Guidance for Windows 10: https://www.ncsc.gov.uk/collection/end-user-device-security/platform-specific-guidance/eud-security-guidance-windows-10-1809
[5] NCSC Commercial Product Assurance for Data Sanitisation: https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?start=0&rows=20&productType=Data%20sanitisation

Server Security

Anti-Virus/Anti-Malware

Required – vendor optional

Preferred Solution: Windows Defender Anti-Virus

Note: If using an alternate AV solution Windows Defender must be present on the endpoint and enrolled into the NHSScotland National Cyber Security Operations Centre (CSOC).

Host Based Firewall

Required – vendor optional

Preferred Solution: Windows Defender Firewall

Operating System Security

Microsoft Security Baselines and CIS recommended secure configurations.

Local Administrator Password management

MS LAPS

Storage Disposal

Faulty and end of life storage solutions are to be shredded or securely wiped using an NCSC certified product and a full audit trail of the process is to be maintained by the local Health Board.

8. Enterprise and Network Security

The enterprise environment must be controlled in compliance with the CRF and NISR.

Enterprise and Network Security

Patch Management (Microsoft & Third Party)

Devices within the scope of the Cyber Resilience Framework should be patched within 14 days of an update being released, where the patch fixes a vulnerability with a severity the product vendor describes as ‘critical’ or ‘high risk’. Out of band patches should be given priority.

For all other equipment the target deployment time for patch management is 2 weeks, with a maximum of 4 weeks, from the date of release.

Scheduled security updates and patches may be excluded if it can be proven that the update will cause issues with critical systems or software

Patch Management Tool

Required – vendor optional

Preferred Solution:
Current Branch Microsoft Configuration Manager with App-V
- Microsoft InTune
- Ivanti Endpoint Security
- Ivanti Security Controls

Network Security

Firewalls with remote monitoring must be in place between internal networks and all external environments, including SWAN, direct ISP Internet, and partner groups such as councils, and other public sector organisations.
Configurations changes in agreement with local Health Board.

Boundary Firewall

Required – Microsoft Azure compliant firewall that is malware aware – vendor optional

Web Filtering

Required – Vendor Optional
Microsoft Productivity Suite should be used where appropriate.

Remote Access

Required – Multi Factor Authentication solution – vendor optional

Multi Factor Authentication

On premises MFA is required and must be agreed at local Board Level

Network Access Control

Required – vendor optional

Penetration Testing

All new systems must have independent, CREST (or equivalent level) certified, penetration testing carried out on them prior to becoming operational.
Penetration testing must be carried out on existing and legacy systems on a regular basis.

9. Network

Recommended specifications for connectivity within premises, between locations and to other networks.

Network

Local Area Network

Minimum: 100Mb/s to wired client devices.
Desirable: 1Gb/s to wired client devices.

Wireless - Local Area Network

Minimum: IEEE 802.11ac
Desirable: IEEE 802.11ax
Secure encryption cyphers and protocols should be implemented i.e. WPA2 enterprise or better. Secure access to be provided for staff and option to allow guest access on a separate VLAN.

Wide Area Network

NHS Scotland sites are connected via SWAN, COIN or SDWAN.
Site bandwidths vary, depending on location, from 10Mb/s to 1Gb/s with 10Gb/s desired at the core.

QoS should be applied end to end and in line with national QoS policies. underlying technologies utilised will be determined by local boards with a view to ensuring latency is kept to a minimum with a target of <20ms for real time applications.

Voice Services

Minimum: Boards should be moving away from traditional PSTN based services onto more modern IP solutions in advance of the scheduled PSTN switch off. Critical services should have a 99.999% availability platform supporting the services.

Desirable: option to utilise physical or soft phones, integration with desktop applications allowing for unified comms. For clarity, there is no intention to forcibly replace existing, physical, handsets with PCs.

Aspirational:

- Omnichannel communication – adapting to modern ways of communication.
- Integration with the national Microsoft tenancy

Alternative solutions: should not result in increased costs or complexity to other NHS Boards.

Video Services

Minimum: Compliance with NHSScotland Video Conferencing Standard (ref 2)
Desirable: Minimum plus MS Teams and room-based integration
Alternative solutions such as Webex should not result in increased costs or complexity to other NHS Boards.

10. Client Management

Client Management

Hardware Asset Management

Required – vendor optional

Preferred Solution: Microsoft Configuration Manager / Enterprise Mobility Suite

Software Asset Management and Licence Metering

Required – vendor optional

Preferred Solution: Microsoft Configuration Manager / Enterprise Mobility Suite

Application Virtualisation

Required – vendor optional

Preferred Solution: App-V (available to all Boards as part of the National MS Licencing agreement)

11. Client Build

Recommended specifications for hardware, operating systems for PCs, laptop, tablet and mobile devices.

Client Hardware

PC Hardware

Processor

UEFI Compliant

Memory
16Gb RAM
Disk Drive
SSD
Tablet & Mobile Device Hardware
Tablet and Mobile Device hardware should be bought from the National contract to ensure that it is the latest compliant model. The devices operating system must be in support and compatible with InTune Mobile Device Management and the device registered at a hardware level with relevant management tools.

12. Server Management

Recommended specifications for hardware, storage, operating systems, databases and web hosting.

- Where there is already an **existing system** in place the instance must be in extended support as a minimum.
- Where a **new build system** is being implemented the instance must be in mainstream support as a minimum.

Server Management
Hardware
As specified by Health Board, either physical or virtual instance
Virtualisation
• **VMWare:** vSphere as per mainstream support matrix • **Hyper-V:** Hyper-V Server as per mainstream support matrix All alternative virtualisation solutions must be in support as per the mainstream support matrix Public Cloud hosted virtualisation solutions should be considered as appropriate and in line with the Cloud First policy.
Storage
As specified by Health Board, either physically attached or SAN Cloud offerings should be considered as appropriate and in line with the Cloud First policy.

Operating System
Windows Server as per mainstream support matrix Red Hat Enterprise Linux: as per mainstream support matrix
Database
SQL Server as per mainstream support matrix Oracle as per mainstream support matrix
Web Hosting
IIS as per mainstream support matrix Apache Tomcat as per mainstream support matrix
Backup and Restore
The Appropriate Recovery Time Objective (RTO) and Recovery Point Objective (RPO) agreements must be in place for critical systems. These should be as specified by the local Health Board, in line with the existing Health Board Business Continuity Planning Strategy and backup policies. It is recommended that immutable copies are created and maintained for all key systems. Restore testing from backups should be completed as part of the end-to-end testing process on any new system and should be completed on a regular basis for business critical systems.

13. On Premise Hosting Environment

Recommended specifications for data centres and computer rooms within Health Boards and beyond.

On Premise Hosting Environment
General
Primary and Secondary (DR) Data Centres sites should be used and regularly tested for failovers.

Resilience

As specified by Health Board but recommended TIA-942 / Uptime Institute Tier-2 availability minimum (with aspects of Tier-3 such as dual PSU's in all servers, storage and networking devices).

Rack

Availability in agreement with local Health Board, specification to Electronic Industries Alliance standard 19" rack mount.

Environment

As specified by local Health Board but recommended:

- N+1 cooling capacity, minimum dual units
- Hot/Cold aisle configuration, maximising power utilisation efficiency.
- Target PUE <1.5

Power

As specified by local Health Board but recommended:

- Dual incoming supplies – N+N capacity
- Dual UPS – N+N capacity
- Each supply has own distribution board
- Each rack is supplied with 32A Commando connection from each supply

Desirable:

- Power Monitoring with separate monitoring for IT Infrastructure and Environmental controls

Access

Physical site and equipment access in line with local Health Board arrangements
Remote support in line with Health Board arrangements and security policies.
Access control policies should be appropriately enforced for each security level.

14. Health Board Naming Conventions

As NHS Scotland moves towards the use of cloud platforms, there is a requirement to ensure Boards use meaningful names when utilising shared cloud services. These names must be unique for each Health Board using a given cloud service; therefore, a naming convention is required. The agreed standard naming conventions specified in the table below must be prefixed to each collaboration item by each individual Boards.

NHSScotland Health Board Naming Conventions	
Golden Jubilee	GJNH
Healthcare Improvement Scotland	HIS
NHS Ayrshire & Arran	AA
NHS Borders	BOR
NHS Dumfries & Galloway	DG
NHS Fife	FIFE
NHS Forth Valley	FV
NHS Grampian	GRAM
NHS Greater Glasgow & Clyde	GGC
NHS Public Health Scotland	PHS
NHS Highland	NHSH
NHS Lanarkshire	LAN
NHS Lothian	LOTH
NHS Education for Scotland	NES
NHS National Services Scotland	NSS
NHS Orkney	ORK
NHS Shetland	SHET
NHS Tayside	TAY
NHS Western Isles	WI
NHS 24	N24
Scottish Ambulance Service	SAS
The State Hospitals Board for Scotland	TSH

East of Scotland Region	EoS
West of Scotland Region	WoS
North of Scotland Region	NoS

National	NHSS

15. Green ICT Compliance

Summary of Legislation and Scottish Government Policy
The Scottish Government Green ICT policy is not itself underpinned by legislation or mandating. It will, however, contribute to the mandatory and reporting elements established in other aspects of Scottish Government Legislation and policy initiatives. NHS Scotland Boards and Suppliers should comply with the following aspects of legislation:

Procurement Reform (Scotland) Act, 2014
The sustainable procurement duty of The Procurement Reform (Scotland) Act, 2014 [6] refers to the environment, and requires authorities to produce procurement strategies and annual reports. The key element pertinent to the Green ICT strategy is that before carrying out a regulated procurement initiative, public authorities should consider how in conducting the procurement process they can improve the economic, social, and environmental wellbeing of the authority's area.

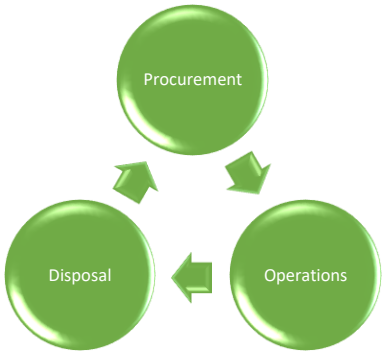
Climate Change (Emissions Reduction Targets) (Scotland) Act 2019
The Climate Change (Scotland) Act 2009 was amended by the Climate Change (Emissions Reduction Targets) (Scotland) Act 2019[7], increasing the ambition of

[6] https://www.gov.scot/publications/procurement-reform-scotland-act-2014-statutory-guidance/
[7] https://www.legislation.gov.uk/asp/2019/15/contents/enacted

Scotland's emissions reduction targets to net zero by 2045 and revising interim and annual emissions reduction targets. The amendments also update arrangements for Climate Change Plans to meet the targets to reduce Scotland's greenhouse gas emissions, in comparison to a 1990-1995 baseline, by at least 75% lower than the baseline by 2030, 90% lower than the baseline by 2040 and reaching Net Zero by 2045. The Act requires Scottish Ministers to set annual targets for Scottish emissions from 2010 to 2050, and publish a report on proposals and policies setting out how Scotland can deliver annual targets for reductions in emissions.

Waste Electrical and Electronic Equipment (WEEE)
The EC Directive on Waste Electrical and Electronic Equipment (2002/96/EC) was made law in the UK IN 2007. The WEEE regulations[8] have interdependencies with the Scottish Landfill Tax[9] which came into force in April 2015, and also with Scotland's Zero Waste Plan[10]. WEEE obligations do not cover all aspects of waste and asset disposal (e.g. data removal and destruction).

The Green ICT Lifecycle:
Green ICT aims at reducing emissions and other waste produced across the ICT lifecycle – from procurement to operational use, to disposal.



Procurement Principles:

- Consider extending life of existing systems
- Go for services not assets: Cloud services, virtualise, consolidate
- Packaging reduction, re-use, repair and re-cycling methods

Operations Principles

- Minimise Power consumption
- Follow data centre standards for efficient operations to help reduce power consumption.
- Develop a roadmap for the transition from hosting own data to hosting in cloud based services to further reduce power consumption

[8] https://www.sepa.org.uk/regulations/waste/waste-electrical-and-electronic-equipment-weee/
[9] https://revenue.scot/taxes/scottish-landfill-tax
[10] https://www.gov.scot/policies/managing-waste/

- Reduce paper consumption
- Embed green behaviours in operational practices and services

Disposal Principles:

- Repair before disposal
- Re-use and refurbish
- Re-cycle in line with regulations
- Clean and re-sell/donate
- Dispose in line with regulations

Environmental Standards and PUE - Energy use and environmental impact:
It is well recognised that data centres are large consumers of energy, the main areas are IT power and ancillary/cooling power. The only credible and widely accepted energy performance rating system for data centres is the Power Usage Effectiveness (PUE) rating where the most efficient score is 1.

The rating is calculated by dividing the total data centre load by the IT load.

PUE Rating	Level of Efficiency
>3	Very Inefficient
2.5	Inefficient
2	Average
1.5	Efficient
1.2	Very Efficient

The Target for Data Centres hosted by NHSScotland Boards is <1.5 PUE

16. Infrastructure Management

The following should be noted in relation to Managing NHSScotland Infrastructure:

- Health Boards manage and operate their infrastructure services locally to ITIL aligned processes.
- Suppliers and their service desks should equally be ITIL aligned.
- Change control or similar requests may require approval by a Board Design Authority or CAB.
- Suppliers should provide sufficient advance notice for planned works so Health Board approval can be agreed.
- Changes should be scheduled for an agreed time that causes least disruption to the business."

Exceptions to the Standard

Where there is a need to deviate from the Infrastructure Standard, then a request must be submitted in writing to the Chair of the National Infrastructure Group. All requests will be considered by the National Infrastructure Group and a written response will be provided outlining the decision.

Governance

Where there is a requirement for approval and sign off various groups and Management Boards exist within NHSScotland. The process to be followed for approval will vary dependent on the financial levels and operational impact of the request.

Digital Health & Care has the following governance structure for infrastructure decision making and sign off:

For Technical Decisions and Assurance:

- The Digital Health & Care Technical Design Authority (TDA) which is commissioned by, and reports into, the Digital Health & Care Strategic Leadership Board
- Digital Health Leads Group
- National Infrastructure Leads Group

For Financial / Funding Decisions:

- Major Programmes Assurance Board - which is commissioned by, and reports into, the Digital Health & Care Strategic Leadership Board
- Digital Health Leads Group
- National Infrastructure Leads Group