NHS
Staffordshire and
Stoke-on-Trent
Integrated Care Board

# Staffordshire and Stoke-on-Trent ICB Information Security Strategy

NHS
Staffordshire and Stoke-on-Trent
Integrated Care Board

# Contents


| | | Page |
|---|---|---|
| | | |
| (1) | Introduction | 3 |
| (2) | National Cyber Security Centre “Ten Steps” Overview and Gap Analysis | 3 – 7 |
| (3) | Network Security | 7 – 9 |
| (4) | Malware and Anti-Virus | 9 – 10 |
| (5) | Boundary Protection | 10 – 11 |
| (6) | Sanitisation, Reuse, Disposal and Destruction of Electronic Media | 11 – 12 |
| (7) | Vulnerability Assessments | 12 – 13 |
| (8) | Identity and Passwords | 13 – 15 |
| (9) | Flexible (Remote / Mobile / Agile) Working | 15 |
| (10) | Incident Management | 15 – 16 |
| (11) | Risk Management | 16 – 17 |
| (12) | Skills and Training | 17 |
| | | |
| APPENDIX ONE: Remote Working Standard Operating Procedure (SOP) | | 18 – 22 |
| | | |

## (1) Introduction

1.1 This Strategy takes forward the predecessor pan-Staffordshire & Stoke-on-Trent CCGs version as part of the ICB's Establishment in 2022. It pulls together the different elements that belong to the ICB and incorporates all systems managed internally and by our IT Service Provider: Staffordshire & Shropshire Health Informatics Service (SSHIS).

1.2 It is based upon industry best practice, as communicated by NHS Digital through their "Good Practice" guides for NHS organisations; and also as communicated by National Cyber Security Centre guidance for the UK as a whole.

1.3 There are elements that cross-reference to the wider digital modernisation strategy being progressed through our Integrated Care System (ICS) Data & Digital Workstream.

1.4 Elements also reference to SSHIS as our IT Service Provider, and the various policies, procedures and strategy documents that apply across their domain. SSHIS are accredited to ISO27001 across their underlying infrastructure.

1.5 Aspects also refer to a range of separate Information Governance (IG), Information Risk and Security issues that are covered within the ICB's approved IG documentation (available on ICB website). Taken together these documents allow the ICB to:

- ☑ Understand cyber security and distil knowledge to all ICB staff and stakeholders
- ☑ Respond to cyber security incidents to reduce the harm they cause
- ☑ Apply industry and academic expertise to nurture the ICB's cyber security capability
- ☑ Reduce risks to the ICB by securing our networks

## (2) National Cyber Security Centre (NCSC) "Ten Steps" Overview

2.1 The "Ten Steps to Cyber Security" published in 2012 is now used by a majority of the FTSE350. They set out recommendations to avoid the worst effects of a cyber-attack and how attackers typically undertake them. Understanding the cyber environment and adopting an approach aligned with the Ten Steps is an effective means to help protect organisations.

2.2 An effective approach to cyber security starts with establishing an effective organisational risk management regime. This regime and the other nine steps that surround it are described below (an infographic from the NCSC describing the steps follows this section). These steps and the related sub-sections provide the core content of this strategy.

### *(i) Risk Management Regime*

Embedding an appropriate regime across the ICB is supported by a separate Risk Management Strategy. This ensures a risk culture is supported by a governance structure that is actively owned by the Board, Executive and Senior Managers. This clearly communicates our approach to Risk Management, under the development of policies and practices. These all aim to ensure that employees, contractors and suppliers are aware of the corporate approach, how decisions are made and any applicable risk boundaries.

### *(ii) Secure Configuration*

Having an approach to identify baseline technology builds and processes for ensuring configuration management greatly improves the security of our systems. Through the main SSHIS Network Security policy, we ensure that unnecessary functionality from systems is removed or disabled, to quickly fix known vulnerabilities (usually via patching through network alerts and system-wide messaging). Failure to do so is likely to result in increased risk of compromise of our corporate systems and information.

***(iii) Network Security (Identity, Passwords and Encryption)***

The connections from our network to the Internet or other partner networks expose our systems and technologies to attack. By creating and implementing appropriate policies and architectural / technical responses, we work to reduce the chances of these attacks succeeding or causing harm. Our network span several sites, the use of mobile or remote working and some “cloud” services, which makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, we also think about where data is stored / processed and where an attacker would have opportunity to interfere with it.

***(iv) Managing User Privileges (Application Security)***

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users are provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges is carefully controlled and managed under the ‘least privilege’ principle.

***(v) User Education and Awareness (Skills and Training)***

Users have a critical role to play in our IT security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisations secure. This is supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious Information Governance culture.

***(vi) Incident Management***

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.

***(vii) Malware and Ransomware Prevention (Anti-Virus Solutions)***

Malicious software (malware) is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact systems and services. The risk is reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence-in-depth' approach.

***(viii) Monitoring and Vulnerability Assessment***

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows us to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is seen as a key capability to comply with NHS / UK legal or regulatory requirements.

***(ix) Removable Media Controls (Boundary Controls + Hardware / Software Security)***

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of data. Our policies are clear about the business need to use removable media and apply appropriate security controls to its use.

***(x) Home and Mobile (Remote) Working***

Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. We have established risk-based policies and procedures that support mobile working or remote access to systems that are applicable to users and service providers (see later section within this document for a policy approach to ensuring staff are aware and trained on the secure use of their mobile devices in the environments they work in).

NHS
Staffordshire and Stoke-on-Trent
Integrated Care Board

National Cyber Security Centre

# 10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

## Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

## User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

## Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

## Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

## Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.


## Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

## Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

## Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

## Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

2.3 The table below provides an initial "Gap Analysis" in response to the "Ten Steps", in terms of what we have got in place now and what we will need to do where not. These will become the priority areas for aligned strategy implementation matters.

| 10 Steps Area & Lead Organisation | What have we got | What do we need (with Responsible Officer & Timescales) |
|---|---|---|
| **Risk Management Regime** (ICB) | • Wider ICB Risk Regime<br>• Wider SSHIS Regime (separate corporate risk register)<br>• Discussed at Service Review meetings with CSU - Shared Risks go to the Intelligent Customer Forum (ICB Lead = Andy Hadley)<br>• See Section #11 | • Full Board awareness of cyber risk – sessions due as part of annual IG refresher training<br>• Specific cyber risks on corporate risk register (Primary Care Digital Programme Lead & ICB IG Lead, ongoing) |
| **Secure Configuration** (SSHIS) | • Regular (monthly) vulnerability scans and security patching<br>• Baseline technology builds for customers (standardised software on desktops)<br>• Inventory of assets (hardware & software)<br>• ICB Information Asset & Information Risk Work Programme and systems (via MLCSU's u-Assure system)<br>• ICB Information Asset Owners & Administrators (IAOs & IAAs) | • No gaps |
| **Network Security** (SSHIS) | • Firewalls at Network Boundary<br>• See Sections # 3 & 5 & 8 | • No gaps |
| **Managing User Privileges** (SSHIS / ICB) | • Service Provider formal procedures for managing and monitoring elevated access rights<br>• Access rights are limited to those requiring them for their duties | • ICB to identify separate applications operating on the Network / Estate |
| **User Education & Awareness** (ICB) | • See Sections # 8 & 12 &16 | • Regular review of user / staff training: re. appropriateness, timeliness (ICB IG Lead, ongoing) |
| **Incident Management** (ICB / SSHIS) | • See Section # 10<br>• SSHIS Disaster Recovery & Business Continuity Plans in place – includes incident management<br>• ICB Business Continuity Plans in place<br>• ICB Incident Management policy | • ICB assurance that plans have been robustly tested (as a maintenance action) – applicable to both service provider and own internal documentation: validation via Data Security & Protection Toolkit (ICB IG Lead, ongoing) |

| Ten Steps Area and Lead Responsible Organisation | What have we got | What do we need (with Responsible Officer & Timescales) |
|---|---|---|
| **Malware Prevention** (SSHIS) | • See Section # 4 | • No gaps |
| **Monitoring & Vulnerability Assessment** | • See Sections # 10 & 11 | • ICB to identify separate applications operating on its Network Estate (if any, and be assured via the DSPT of any activities required to show DSPT Assertion compliance – annual / ongoing process) |
| **Removable Media Controls** (SSHIS / ICB) | • Implement Port Control<br>• All removable media is encrypted<br>• All data is securely wiped from removable media<br>• See Section # 6 | • No gaps |
| **Home / Mobile /Remote Working** (ICB / SSHIS) | • SSHIS multi-factor education (SSHIS) utilising Microsoft Direct Access technologies<br>• ICB – see policy Appendix One | • No gaps (technology element)<br>• ICB – policy approval and implementation supported by regular staff training & awareness (ICB IG Lead, ongoing) |

## (3) Network Security

*[As adapted from the NCSC's "Ten Steps" concerning Network Security matters]*

The connections from our networks to the Internet and other partner networks expose our systems and technologies to attack. By creating and implementing appropriate policies, architectural and technical responses, we can reduce the chances of these attacks succeeding or causing harm.

Networks need to be protected against internal and external risks or threats, such as:

- *Exploitation of Systems:* ineffective network design may allow an attacker to compromise systems that perform critical functions, affecting our ability to deliver essential services or resulting in severe loss of customer or user confidence
- *Compromise of Information:* poor network architecture may allow an attacker to compromise sensitive information in a number of ways: they may be able to access systems hosting sensitive information directly or perhaps allow an attacker to intercept poorly-protected information whilst in transit (e.g. between our end-user devices and a cloud service)
- *Import / Export of Malware:* failure to put in place appropriate security controls could lead to malware and the potential to compromise ICB business systems; or conversely, users could deliberately or accidentally release malware or other malicious content externally with associated reputational damage
- *Denial of Service:* internet-facing networks may be vulnerable to Denial Of Service (DOS) attacks, where access to services or resources are denied to legitimate users
- *Damage or Defacement of Corporate Resources:* attackers that have successfully compromised the network may be able to further damage internal and externally facing systems / information; such as defacing our websites, or posting onto our social media accounts, harming the organisation's reputation and customer confidence

**How we will manage the risk:**

- ☑ Ensuring that SSHIS continues to produce, implement and maintain network security designs and policies that align with the ICBs' broader risk approach – for example ICB attendance at Intelligent Customer Forum. Through this, the ICB will liaise with SSHIS to ensure that they as our IT supplier use recognised network design principles based on Cisco Certified inter-Networking Expert (CCIE) accredited guidelines to help define appropriate network architecture, including the network perimeter, any internal networks and links with other partner organisations.

- ☑ Ensuring that SSHIS continues to manage the network perimeter (access to ports, protocols and applications) by filtering and inspecting all traffic at the network perimeter to ensure that only traffic which is required to support the business is being exchanged. Procedures to control and manage all inbound / outbound network connections and associated technical controls to scan for malicious content will continue to be deployed.

- ☑ Ensuring that SSHIS continues to use firewalls to create a buffer zone between the Internet (and other untrusted networks) and networks used by the ICB. The firewall rules set are expected to deny traffic by default and a "white-list" applied that only allows authorised protocols, ports and applications to exchange data across the boundary. This will reduce the exposure of systems to network-based attacks. Effective processes for managing changes to avoid workarounds will continue to be developed and implemented.

- ☑ Ensuring that SSHIS continues to prevent malicious content, by deploying malware checking solutions and reputation-based scanning services to examine both inbound / outbound data at the perimeter, in addition to protection deployed internally.

- ☑ Ensuring that SSHIS continues to protect the internal network, by ongoing implementation and management of current firewall technologies.

- ☑ Ensuring that SSHIS continues to secure wireless access: all wireless access points should be appropriately secured, only allowing known devices to connect to corporate Wi-Fi services.

- ☑ Ensuring that SSHIS continues to enable secure administration and Administrator access to any network component through proper authentication and authorisations processes; and ensure that default administrative passwords for network equipment are changed.

- ☑ Ensuring that SSHIS continues to monitor the network via appropriate intrusion detection and prevention tools and by qualified staff. These capabilities will monitor all traffic for unusual incoming / outgoing activity that could be indicative of an attack. Alerts generated by the system will be automatically logged and managed by the SSHIS Service Management Tool (SMT).

- ☑ Ensuring that SSHIS continues to conduct regular penetration tests of the network architecture and undertake simulated cyber-attack exercises to ensure that security controls have been well implemented and remain effective.

These are all covered by a separate SSHIS Network Security Policy. This sets out the policy for the protection of the confidentiality, integrity and availability of the network covering all SSHIS customers across the Staffordshire & Shropshire ICS, and establishes the security responsibilities for network security.

The objective is to ensure the security of the network, ensuring that it is available for users and to preserve its integrity, confidentiality, assets protection and protect the network from unauthorised or accidental modification. It also ensures the proper use of the network and makes users aware of what the ICB-ICS and SSHIS deem as acceptable and unacceptable use of its networks.

It also covers explicit provision for the following:

- Access to the network is via a secure log-on process, designed to minimise unauthorised access
- Access is gained in a number of flexible ways, including the ability to access systems[1] remotely
- Each is managed and governed by their own policies / procedures
- There is a formal, documented user access registration / de-registration procedure (ICB lead)
- ICB must approve user access prior to this being processed by the SSHIS Service Desk
- Access is not granted until the SSHIS Service Desk registers a user
- Access rights are allocated on the requirements of the user's job role, rather than on a status basis
- Security privileges (i.e. 'Super user' or admin rights) are similarly allocated
- All network users have their own individual user identification and password
- All users are required to change their password (frequency / complexity as per Information Security policy approach set out in the ICB Staff IG Handbook)
- Network accounts are subject to a lockout policy
- User access rights will, upon notification from line managers, be immediately removed or reviewed for those users who have left the organisation or changed jobs
- There is a documented procedure to identify and disable redundant accounts i.e. accounts that have not been accesses for a specified period of time

## (4) Malware and Anti-Virus

This section focusses on the key points of NHS Digital's Cyber & Data Security Good Practice guidance series on how the ICBs should protect their networks and systems from malware by implementing and managing Anti-Virus and Malware Solutions and educating staff as service users to recognise and deal with malware.

*Note: as ICB is classed as smaller organisation that uses a third party IT service provider (SSHIS), the contents of this section may be used to ensure that the contract with them covers the required anti-virus and malware response.*

Increasingly viruses and malware are being used in criminal or disruptive attempts to compromise an organisation's systems, or to gain unauthorised access to information and to take control of computer resources. Often these are done for the purposes of redirecting these to attack other intended targets through propagation of malware. For the purposes of this section, Malware is defined as computer Viruses, Worms, Trojans and Spyware[2].

[1] E.g. Virtual Private Network (VPN) providing access to the Community of Interest Network (COIN); Microsoft Unified Access Gateway (UAG), providing secure access to systems and VPN solution; McAfee Enterprise Mobility Management, providing secure access to email on mobile devices; Microsoft Direct Access, providing secure remote access.

[2] A 'Virus' is a type of malware which infects files on a computer system. A virus may look for specific types of file to infect such as Word documents; once an infected document is sent to someone else; the virus then spreads to and infects that person's computer. A resident computer virus can survive system reboots and operates in the background on the system, looking for files to infect. A non-resident computer virus only runs when an infected file is launched. // A 'Worm' is a type of malware which does not require user interaction to run. They can spread from system to system utilising automated infection methods (i.e. it can replicate itself and take advantage of automatic file sending / receiving features on the computer) and generally exploit unpatched software vulnerabilities in order to spread. A worm does not steal personal information from systems, but may simply exist to spread and cause system problems in relation to integrity and availability. // A 'Trojan' is malware which on the surface has a legitimate usage but unbeknown to the user contains functionality which can be used to steal sensitive data or perform other unwanted actions.// 'Spyware' is software that aims to gather information about a person or organisation, often without them being aware of it, that sends this information to another entity without the user's consent. Spyware asserts control over a device without the user's knowledge, or it may send such information with consent through the use of "cookies". Spyware is adware, system monitors, tracking cookies and Trojans, but also include digital rights management capabilities that route back to the other entity applying spyware to the system.

The best defence against these is to combine a range of technical Anti-virus and Malware software solutions, with robust security policies / procedures and effective staff / user education and awareness programmes to stop malware from infecting our systems.

Our Anti-Virus and Malware Solutions are hosted by our third party IT service provider (SSHIS), and is scaled to the needs of the ICBs as applicable to their size and scale. As a minimum, these solutions include:

- Software deployment on desktops, laptops and servers connected to the network or the Internet;
- 'On Access', 'On Demand' and 'Scheduled' Scanning;
- Automatic updating of definitions and engines;
- Integration with email and messaging services;
- Logging of all relevant events;
- Restricting change of software configuration settings to authorised personnel only; and
- Memory resident scanning provides protection for users from external threats such as malicious sites on the Internet

Anti-Virus and Malware solutions provide the ability to carry out regular scans on at least a weekly basis and consist of a full scan of all areas of the machine. This provides a consistent baseline of protection (mostly scheduled to run outside of normal office hours or at a time which will not disrupt normal working). The use of 'Heuristic' scanning, where the ability of the anti-virus software to detect patterns of behaviour on the machine which may represent virus or malware like activities, is also deployed to further increase the protection that the software can provide.

Active and Passive Network Monitoring of user machines provides further protection against malicious processes. If an application demonstrates behaviour indicating the presence of malware, Active Monitoring software can prevent the application from starting.

User Education is critical to our organisational security approach for the prevention of malware incidents.

System users are routinely educated through awareness-raising to recognise suspicious behaviour, not to open suspicious attachments from unknown senders, not to attempt to circumvent network technical solutions by downloading / installing unapproved software to corporate hardware (supported by policies preventing software addition without admin rights), not to visit websites designed to spread malware and a vigilance culture of reporting any suspicions relating to viruses or malicious software to the SSHIS Service Desk / IT Department immediately.

Education is an ongoing activity that begins when a new employee joins the ICB. Multiple methods exist, including standardised or ad hoc communications methods and formal IG training sessions. Such education links in with the ICBs' IG Handbook and associated policy statements on anti-virus and malware, acceptable use, remote working, removable media etc.

## (5) Boundary Protection

This section focusses on the key points of NHS Digital's Cyber & Data Security Good Practice guidance series on how the ICBs should implement an organisation-wide boundary protection scheme that will enable them to have procedures / processes in place that will enable them to:

- *Successfully and securely configure systems, devices and software across networks*
- *Successfully and securely lockdown systems, devices and software across networks*
- *Successfully and securely manage gateways to other networks*
- *Successfully and securely monitor networks and react to incidents*

*Note: as ICB is classed as a smaller organisation that uses a third party IT service provider (SSHIS), the contents of this section may be used to ensure that the contract with them covers the required response.*

IT networks provide many benefits, like enabling organisations to quickly / efficiently share information, enabling collaboration, using powerful data processing tools and allowing organisations to store large amounts of data that can be accessed quickly. However they also create security risks. These include greater vulnerability to access from both inside and outside the ICB, where people may not have authorisation to access data, information or systems.

The risks include theft, loss, compromise or corruption of data, the loss or limited availability of IT systems, data or processing tools, the inability to communicate or ultimately the inability to carry out core business functions. Implementation and management of strong boundary protection goes some way to mitigate these risks.

### (a) Configuration

Network and system configuration control is essential to ensure unauthorised changes are detected or cannot take place. All security settings must be documented and understood; and where changes are necessary, a detailed and rigorous change control process followed (for procedural and technical measures) to ensure all changes are fully documented and approved.

Our networks should be configured and security-hardened to ensure that services that may be exploited by an attacker are disabled or kept to a minimum. This includes lock-down of network connected devices in line with organisational policy and guidance; with all software and hardware configured securely during installation and then patched regularly.

To help this, the latest versions of software, service packs and security updates are deployed across the network at the earliest opportunity. System users are generally not permitted to install software that is not controlled or supported by our IT service provider.

### (b) Patch Management

New vulnerabilities in software and firmware are discovered and reported on a daily basis and security updates, which aim to fix them, should be applied as soon as is reasonably possible by:

- An up-to-date Patch Management policy that sets out the principles for applying patches / updates
- Testing patches before application against Network configuration and software build
- Alternatives to unsupported software where available, with risk assessment / mitigating measures
- Regular IT Health Check assessments to help identify known vulnerabilities

## (6) Sanitisation, Reuse, Disposal and Destruction of Electronic Media

This section focusses on the key points of NHS Digital's Cyber & Data Security Good Practice guidance series on how the ICB should implement organisation-wide, robust and fit for purpose systems for the sanitisation, reuse, disposal and destruction of IT and electronic media. This guidance will enable the ICB to have procedures and processes in place that will enable it to:

- *Successfully and appropriately sanitise media according to the sensitivity and/or classification of data*
- *Successfully / securely reuse electronic media without putting data at risk of being breached*
- *Successfully and appropriately dispose of / destroy electronic media according to the sensitivity and/or classification of the data stored on it*

*Note: as ICB is classed as a smaller organisation that uses a third party IT service provider (SSHIS), the contents of this section could be used to ensure that the contract with them covers the required response. This is undertaken solely by the SSHIS on behalf of the ICB and no third parties are otherwise involved in the process, beyond collection of old items of decommissioned hardware. ICB assets (largely paper-based) are managed through the ICB premises landlord under separate contracts and retained assets are archived with the ICB's supplier.*

## (7) Vulnerability Assessments

This section focusses on the key points of NHS Digital's Cyber & Data Security Good Practice guidance series on how the ICBs should plan these to enable them to:

- *Successfully scope, implement and manage vulnerability assessments across the organisation*
- *Ensure that networks, systems and services are securely configured*
- *Ensure that networks, systems and services are securely locked down*

*Note: as ICB is classed as a smaller organisation that uses a third party IT service provider (SSHIS), the contents of this section may be used to ensure that the contract with them covers the required response.*

A range of vulnerability assessments are available to be performed dependent upon the service or infrastructure in question. This section outlines the types available and suggests when each may be appropriate. It also outlines the various roles and responsibilities of the organisation's staff, vulnerability assessment providers and other third parties when scoping, preparing and running assessments and during post-assessment reporting.

The purpose of an Infrastructure vulnerability assessment is to ensure that any significant new infrastructure is installed in an appropriately secure manner or that when existing infrastructure undergoes a significant change that vulnerabilities are not introduced. Infrastructure usually means includes servers, switches, routers, databases, firewalls, etc and are mostly covered under the terms of the IT contract held with the SSHIS.

The scope of the assessment is usually very prescriptive, identifying the specific hosts that are to be assessed and instructing that no other infrastructure should be investigated. In addition, those carrying out the assessment are usually under instruction not to attempt to exploit any vulnerability discovered if there is a possibility that doing so might affect services running on that host.

This ensures that the assessment informs on vulnerabilities, while offering the best assurance that adjacent (and possibly live) services are unaffected. So while each should be scoped individually, each assessment may include, but is not limited to the following:

- Network port scanning + vulnerability scanning
- Manual testing
- On-host auditing
- Web server scanning
- Basic database checks

They can also be used to ensure that there are no obvious security holes or vulnerabilities within the application that would allow an unauthorised user access to the data or underlying infrastructure (Operating System or Database) via a flaw with the application code.

They can also include the assessment of non-human interfaces, commonly submission of data. This assessment is performed to ensure that it is not possible, via the manipulation of data fields, to return inappropriate information or cause a denial of service to the receiving application.

ICB vulnerability assessments will be performed by our third party IT service provider SSHIS and scoped / arranged by them. They will be performed once the infrastructure / application is configured as close to a 'Live' state as possible; and will typically take place in a test environment so as to avoid any possibility of corrupting live data or systems.

There are also regular (monthly) vulnerability assessments completed on the infrastructure and reported to the ICBs by our service provider SSHIS.

## (8) Identity and Passwords

***Identity and Access Management Procedures and Controls***

*Note: as ICB is classed as a smaller organisation that uses a third party IT service provider (SSHIS), the contents of this section may be used to ensure that the contract with them covers the required response.*

If passwords are badly designed or access management controls poorly implemented, they can give attackers an easy way to gain access to systems that could appear legitimate. The security of all the aspects of identity will be checked to ensure that any new user is who they say they are, and the level of given is commensurate with their personal / professional background and applied using the principle of least privilege to limit access or functionality.

Identity and access management refers to the collection of corporate and third party IT service provider based policies, processes and systems that support staff and set permissions within our system: e.g. to perform functions, access corporate data / records and system administration.

The access management system is comprised of a number of technical components, including directory services and authentication / authorisation. These provide the overall strategy governing who is authorised to access systems, data or functionality, how users request access, when access should be revoked and whether particular operations require multiple users to collaborate.

Operations and monitoring supporting processes / technology help identify and enable investigation of any breaches of policy or controls. They also determine how the identity of a person is established, both at point of first contact and subsequent interactions with ICB systems or processes. Privileged user management is deployed to gain additional controls to safeguard the most sensitive operations.

***SSHIS Access Management Policy***

Formal user access control procedures are documented, implemented and kept up to date for the ICB's network and wider SSHIS domain to ensure authorised user access and to prevent unauthorised access. This covers all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.

Each user is allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform
- Requires a unique login that is not shared with or disclosed to any other user
- Requires an associated unique password that is requested at each new login

System administration accounts are only provided to users that are required to perform system administration tasks and are managed in accordance with a separate Elevated User Rights Policy. SSHIS maintains software that automatically creates an account in Active Directory (AD) when a new member of staff is entered onto the Electronic Staff Record (ESR) system. The AD account is matched using the staff Assignment Number in ESR.

For non-salaried staff, a request for access to the network is submitted to the SSHIS IT Service Desk via the Service Management Tool (SMT). Applications for access are only submitted via the online Network Request application by a Line Manager or nominated representative with a valid network account. The SSHIS does not validate the requesting manager`s authority, but does record an audit trail of the requestor.

When an employee leaves the organisation, their access to computer systems and data must be suspended at the close of business on the employee's last working day. For salaried staff, their network account is linked to the ESR system, and the end date of the network account is synchronised with the end date on ESR. Once this date has been reached, the account is no longer accessible and processes are in place to remove it from the network. For non-salaried staff, suspension of access rights is similarly undertaken via the SMT, in line with the Leaver Checklist.

***Password Protection***

It is of the utmost importance that passwords remain protected at all times. A separate Password Policy is in place across the wider system and agreed with the SSHIS customers collectively. This requires passwords to be changed at regular intervals, be of an agreed minimum length and meet complexity requirements. User accounts are also locked after a stipulated number of failed logins.

***Privileged User Management***

Anyone with access that enables them to affect change which would be felt beyond their immediate job role could be considered a privileged user (e.g. administering systems or networks which are business-critical; or in accessing systems used to perform a critical function).

SSHIS has a separate Elevated User Rights Policy to define the criteria for which Domain Administrator, Administrative Support or Local Administrative rights for all end-user devices and infrastructure managed by SSHIS shall be granted and managed.

The granting of Administrative Rights Access to desktop, laptop, other EUD, network equipment or server infrastructure is a privilege only provided to individuals who require this level of access and control in order to do their jobs effectively. The policy describes the limited circumstances under which admin rights shall be granted, since these allow users the ability to change standard desktop configuration settings, install software and access and update security settings, potentially creating security weaknesses which could have serious implications for the IT environment.

The SSHIS and the ICBs strictly adhere to the principle of 'Least Privilege' when granting rights to desktop and laptop computers used across the network. Rights will only be granted under the condition that they are essential for the performance of the grantee's job. Lack of adherence to all IT policies may cause revocation of these rights.

Elevated rights will in the majority of cases be granted and actioned by the Network & Systems Manager for SSHIS staff. If a user requires elevated rights they log a ticket on the Service Management Tool (SMT) with the type of access required, together with justification and where possible authorisation from the user's Line Manager.

Such authorisation does not necessarily mean rights will be granted as the Network & Systems Manager reserves the right to refuse requests where there is deemed to be insufficient justification.

***Password Policy***

Formal user password policies and control procedures for the ICBs are implemented and kept up to date within separate IG documentation such as the Staff IG Handbook and Data Security & Protection Policy. This established key principles about password management and integrity (e.g. advice about setting appropriately strong passwords and other key do's and don'ts):

- Passwords should be a combination of letters / digits of a pre-determined length and combination of characters, typically using the lower case of the keyboard
- Passwords and/or PINs should not normally be written down, but if unavoidable, should be held on a secure drive in a passwords folder and never kept with the device or in an easily recognisable form

## (9) Flexible (Remote / Mobile / Agile) Working

*Note: as ICB is classed as a smaller organisation that uses a third party IT service provider (SSHIS), the contents of this section may be used to ensure that the contract with them covers the required response.*

Mobile working and remote system access offers great benefits, but exposes new risks. It extends the transit and storage of information or operation of systems outside of corporate infrastructure, typically over the Internet. Mobile devices will also typically be used in spaces that are subject to additional risks such as oversight of screens, or the theft / loss of devices. Sound mobile working and remote access practices are required to prevent vulnerability to the following risks:

- Loss or theft of the device: mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems; they are often used in open view in locations that cannot offer the same level of physical security as ICB premises
- Being overlooked: some users will have to work in public spaces where they may be vulnerable to being observed when working: this can potentially compromise sensitive information or authentication credentials
- Loss of credentials: if user credentials such as username, password etc are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on / accessible from that device
- Tampering: an attacker may attempt to subvert security controls on the device through the insertion of malicious software or hardware if the device is left unattended; this may allow them to monitor all user activity on the device, including authentication credentials

A separate mobile working Standard Operating Procedure (SOP), provided as Appendix One, determines the processes for authorising off-site work, device support, the type of information or services that can be accessed or stored on devices and the minimum procedural security controls. Risks to the corporate network or systems from mobile devices should be regularly assessed and increased monitoring on all remote connections / the systems being accessed.

All users receive training on the use of their mobile device for the locations they will be working in. Users are required to look after their mobile device and operate securely by following clear procedures set out in Staff IG documentation, which includes directions on:

- Secure storage + management of user credentials
- Incident reporting
- Environmental awareness (the risks from being overlooked etc

## (10) Incident Management

*Note: as ICB is classed as a smaller organisation that uses a third party IT service provider (SSHIS), the contents of this section may be used to ensure that the contract with them covers the required response.*

IT security incidents will inevitably happen and will vary in their impact. Establishing an effective incident management policy and process helps improve resilience, support business continuity, improve confidence and potentially reduce impact. All incidents need to be managed effectively, particularly those serious enough to warrant invoking business continuity or disaster recovery plans. The ICBs' capability to detect, manage and analyse IT security incidents help to minimise:

- Managing business harm: failure to realise that an incident is happening or has occurred limits the ability to manage it effectively, potentially leading to a much greater overall impact (e.g. significant system outage or serious financial loss)
- Continual disruption: not addressing the root cause of incidents (e.g. poor technology or weaknesses in corporate security) could risk exposure to repeated or continual system compromise or disruption
- An incident resulting in the compromise of sensitive information covered by mandatory reporting requirements, which could lead to legal or regulatory penalties

Incident response capability as covered by separate ICB policies help to address the full range of incidents that could occur and set out appropriate responses to these. These define the supporting legal or regulatory reporting requirements, training requirements and the required roles / responsibilities of specific individuals and/or suppliers to handle incidents and provide them with clear terms of reference to make decisions in order to manage any incident.

A data recovery capability is critical to these from an IT perspective. Data losses can occur and so a systematic approach to the backup of essential data is implemented through ICB and SSHIS Business Continuity Plans. Physical backup media are held in a physically secure location, and the ability to recover archived data for operational use is regularly tested.

The root cause analysis of post-incident evidence helps to understand the sequence of events that led up to the incident and may also potentially support any follow-up disciplinary or legal action that may be required as necessary. A "Lessons Learned" review also assesses the performance of the incident management process post-incident to see what worked well and what could be improved.

All ICB Staff are aware of their responsibilities and how they can report and respond to incidents. They are also encouraged to report any security weaknesses or incident as soon as possible, without fear of recrimination. All criminal incidents relevant to law enforcement (e.g. potential or actual cyber-crime is reported to Action Fraud and any other relevant law enforcement agency).

## (11) Risk Management

*Note: as ICB is classed as a smaller organisation that uses a third party IT service provider (SSHIS), the contents of this section may be used to ensure that the contract with them covers the required response.*

Taking risk is a necessary part of doing business, in order to create opportunities and help deliver corporate objectives. For any organisation to operate successfully, it needs to address risk and respond proportionately and appropriately to a level consistent with what risks are willing to be taken or not tolerated. It is important that we apply a similar level of rigour to assessing the risks to technology, systems and information assets as we would to any other risks.

Our established governance frameworks and Risk Strategy enable and support a consistent approach to Risk Management, with ultimate responsibility residing at Board level. The Strategy includes provisions to cater for the organisational "Risk Appetite", which broadly determines what risks the ICB is willing to tolerate and what is unacceptable in pursuit of our business objectives.

Supporting policies have been created within the ICB's IG documentation, which set out the Board-level responsibilities and staff accountabilities (under the SIRO Framework requirements established by the NHS Data Security & Protection Toolkit response to UK GDPR). These help to communicate and support all IM&T risk management objectives. Staff are also made aware of their individual and collective responsibility to help manage security risks across the ICB. Appropriate training that is relevant to their role is undertaken and refreshed annually with IG training.

## (12) Skills and Training

Similar to the previous section about risk and awareness / ownership requirements, including IG training, our staff are central to our ability to operate securely. All staff have the information, knowledge, and skills they need to support the security of networks and information systems. Security awareness and training programmes recognise and are tailored to reflect the way staff really work with security in an organisation, as part of creating a positive security culture.

Training and awareness activities through annual and ongoing IG refresher training (with enhanced specialist training for Information Asset Owners / Administrators) provide appropriate cyber security skills for the job role as undertaken.

Our overall aim is to create a positive security culture, where people are aware of their role in maintaining security and actively contribute to improving organisational IT security. This enables people to make the right cyber security decisions, supported by effective communications on cyber security matters and network / information system security and how these relate to their jobs.

Through separate Data Security & Protection policy and other IG documentation, we support employees with the right tools to promote awareness of the following:

- Removable media and devices policies to help avoid the inadvertent import of malware or compromise of sensitive information
- Fostering an incident reporting culture and regular dialogue to uncovering near misses and areas where technology / processes can be improved, as well as reporting actual incidents
- Security Operating procedures are balanced to support system users in performing their duties while not making security a blocker and therefore possibly ignored
- The risks of external attack such as phishing attempts that rely on taking advantage of legitimate user capabilities / functions
- The risks of insider threat posed by vulnerability to releasing personal or sensitive commercial information to others, or the risk of dissatisfied employees potentially trying to abuse system privileges, or steal / physically deface computer resources
- Staff induction processes for (including contractors or third party users) to make new starters aware of their personal responsibility to comply with corporate security policies,
- Regular IG refresher training for all staff on the security risks facing ICB / the wider NHS
- Promotion of an open incident reporting culture that empowers staff to voice their concerns about poor security practices and security incidents to senior managers, without fear of recrimination
- A formal disciplinary process that reminds staff that any abuse of the ICB's security policies will result in disciplinary action being taken should these be consciously breached, with contractual terms & conditions formally acknowledging / supporting any subsequent disciplinary action.

## Appendix One – Remote / Agile Working Standard Operating Procedure (SOP)

### (1) Introduction

1.1 This Standard Operating Procedure (SOP) applies to NHS Staffordshire and Stoke-on-Trent ICB.

1.2 It has been developed to ensure that those with a business requirement can access the ICBs' systems remotely or use mobile devices in stand-alone mode and without introducing unacceptable threats to the processing of information or networked systems. Remote access is a method of accessing files / systems that can only usually be accessed from an NHS site or by using an authorised Virtual Private Network (VPN) token.

1.3 Remote access to systems is now seen as an important way of working. Remote working can only be undertaken with the use of mobile devices purchased through the Staffordshire & Shropshire Health Informatics Service (SSHIS). Personal devices are not permitted to be used for work purposes other than expressly permitted by the relevant 'Data Controller' and in accordance with the ICB's separate Information Governance policies.

1.4 Critical business processes rely on easy / reliable access to information systems, and securing remote access benefits are considerable, meaning ICB business can be conducted remotely with confidence and sensitive information confidentiality remains assured. This SOP sets out the processes for holding, obtaining, recording, using and sharing information by remote access via the use of mobile devices and includes a set of common controls, which can be applied to reduce the risks associated with remote access.

### (2) Policy Statement

2.1 The purpose of this SOP is:

- To identify and provide effective controls and processes for secure / resilient remote access to ICB information systems, in line with Information Security documentation
- To ensure the confidentiality and security of information accessed via remote access
- To ensure that information security is maintained when users access data on mobile devices
- To ensure the processing of information is operated in accordance with national guidance and local organisational policies
- To ensure that all staff are aware of their responsibilities, comply with the SOP and that the areas covered within it are part of organisation-wide Information Governance (IG) resources

2.2 This SOP forms part of an overall suite of ICB Information Governance documentation, and must be read in conjunction with these. Failure by any employee to adhere to it and its guidelines will be viewed as a serious matter and may result in disciplinary action.

### (3) Definitions

3.1 "User" – anyone who makes use of the ICB's network or computing facilities in order to gain access to systems and applies specifically to:

- All ICB employees, whether at base, travelling or offsite (e.g. staff working at home, or across sites or temporarily based at other locations)
- Any authorised individual using organisational systems: e.g. a trainee, student, contractor / third party organisation with appropriate authorisation to access ICB information assets or infrastructure, volunteer or otherwise

3.2 "The Organisation" – means the ICB.

3.3 "Mobile Devices" – includes but is not limited to portable computers such as laptops, notebooks, tablets, mobile telephones, blackberries and smart phones. All ICB-owned mobile devices must be registered with the SSHIS (via the Service Desk). No mobile device shall store person-confidential information.

## (4) Remote Access Process

4.1 This applies to any technology that enables users to connect organisation-owned systems from geographically dispersed locations. This includes users who use a 'store and forward' option to access data securely stored on a mobile device, which is then synchronised with the live system when returning to base. Remote access is typically over a wireless, General Packet Radio Services (GPRS), 4G or broadband connection. It can include Wide Area Network (WAN) connections.

4.2 It is the responsibility of the relevant Head of Department / Service to submit a request for remote access on behalf of their staff. Applications for remote access should be submitted via email to the SSHIS Service Desk for technical approval, using the Application for Remote Access form at the end of this SOP.

4.3 Each application must include reasonable justification for users to have remote access to systems, outlining the high-level requirement for each request. Each application will also clearly ensure that appropriate awareness of risks are understood and owned by proposed users submitting the application.

4.4 All users are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources; and must notify the SSHIS immediately of any security incidents and/or breaches in accordance with the Information Security and ICB Incident Reporting Policies.

## (5) Accessing Information Remotely

5.1 Access to networks via ICB-owned devices is available via Microsoft Direct Access, a VPN technology utilising both device-based certificates as well as Active Directory user authentication methods. Users are able to access email and applications from any device on the Internet no matter if it is managed or not.

5.2 VPN connectivity is available via Direct Access without the need for a token – these devices are verified as valid endpoints whose identity, service pack level, AV compliance and ownership can be verified. Access from non-ICB devices is provided with Cloud PC, thus leaving no data footprint on the client device.

5.3 Mobile Device Management is provided via Microsoft InTune where Customer licensing allows and Microsoft ActiveSync where licensing is not available. Both solutions allow for device policies to be pushed enforcing device encryption as well as providing remote wipe functionality should a device be lost or stolen.

5.4 Further information can be found within the ICB's Information Security Policy (which can be obtained on the Staff Intranet, ICB website or from the ICB Operational IG lead).

## (6) Mobile Device Security

6.1 Any problems that arise with remote access or mobile devices should be reported to the SSHIS Service Desk. Remote access and encryption queries can only be supported within the SSHIS Service Desk opening hours: Monday to Friday 8.30am to 5pm.

6.2 Mobile devices must never be left unattended in cars or easily accessible areas to reduce the risk of opportunistic theft. If possible, devices should be kept securely locked away when not in use. Care should also be taken during transit. Heavy jolts to a mobile device could cause damage to the hard disk and render the system inoperable.

6.3 Virus Protection software must be installed, active and up to date. Users must routinely connect to the network to ensure the most up-to-date software is installed. For iPads and iPhones, the latest versions of system software must be installed: further advice can be provided by the ICB's Information Governance Lead.

6.4 Staff should also refer to the ICB's Information Security Policy.

## (7) Appropriate Use of Mobile Devices

7.2 Unauthorised software must not be installed on any equipment, including mobile devices.

7.3 Person-confidential information must not be sent via email unless this fully complies with the ICB Policy on Internet and Electronic Mail.

7.4 NO other person (including family members) should be able to overlook what data is being accessed by the user. If a laptop is left for even a short time whilst working, then it must be screensaver locked or the user can press Ctrl+Alt+Delete / Enter or the Windows key + L to lock their screen.

## (8) Responsibilities

8.1 The CEO is ultimately responsible for ensuring that remote access by staff is managed securely.

8.2 The ICB IG Group (accountable to Audit Committee) will maintain policy, standards and procedures for remote access and use of mobile devices and ensure that risks are identified / appropriate controls implemented to reduce those.

8.3 SSHIS will ensure that organisational end systems are securely maintained.

8.4 All staff with remote access and/or use mobile devices are responsible for complying with this SOP and associated standards. All staff must safeguard organisational equipment and information resources; and immediately notify of any security incidents or breaches.

8.5 All users must ensure they seek the necessary security guidance, awareness and where appropriate training to ensure they are aware of their security responsibilities. Irresponsible or improper actions will result in disciplinary action.

8.6 Users must return all relevant equipment (including software) to their Line Manager when remote access and/or the mobile device are no longer required.

## (9) Monitoring Compliance

9.1 To ensure the most comprehensive level of protection possible, every network should include security components that address the following five aspects of network security.

9.2 User Identity – all remote users must be registered and authorised. Local audits of remote access will ensure that authorised users still require their access. User identity will be confirmed by User ID and password authentication. SSHIS is responsible for ensuring a log is kept of all user remote access.

9.3 Perimeter Security – SSHIS will be responsible for ensuring perimeter security devices are in place and operating properly. Perimeter security solutions control access to critical network applications, data and services so that only legitimate users / information can pass through the network. Routers and switches handle this with access control lists and by dedicated firewall appliances.

9.4 Remote Access Systems with strong authentication software control remote dial-in users to the network. A firewall provides a barrier to traffic crossing the network's perimeter and permits only authorised traffic, according to a pre-defined security policy. Complementary tools, such as virus scanners and content filters, also help control network perimeters.

9.5 Security Monitoring – Network vulnerability scanners will be used to identify areas of weakness, and intrusion detection systems to monitor / reactively respond to security events as they occur.

9.6 Remote Diagnostic Services / Third Parties – suppliers of central systems or software that require access to their systems in order to investigate or fix faults will be allowed through remote N3 connection and secure one-time password token.

9.7 Each supplier or user requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified representatives. Each request for dial-up access will be authorised by approved SSHIS staff, who will only make the connection once satisfied of the need.

9.8 Encryption Software – all mobile devices must have appropriate encryption software installed.

## (10) Training Requirements

10.1 It is the responsibility of the ICB to ensure that relevant training on security / confidentiality is readily available, and also to proactively encourage compliance with all aspects of IG or Information Security policy.

10.2 All new starters will undertake IG training as part of their induction; preferably face to face or via e-learning as a safeguard, as per ICB IG policy. A register will be maintained of staff completion of IG training. Line Managers must ensure that all staff complete annual IG training as part of their statutory & mandatory training requirements.

## (11) Equality & Diversity Statement

11.1 The ICB aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

11.2 This SOP has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the “Protected Characteristics” of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. This SOP has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

*Application Form for Remote Working*

[TO BE INSERTED ONCE DEVELOPED]