**Joined Up Care Derbyshire**

**Cyber Security Strategy**

**2023-2026**

**Document control**

|  |  |
| --- | --- |
| **Title** | Joined Up Care Derbyshire Cyber Security Strategy |
| **Authors** | Alvaro Pancisi |
| **Consultation** | Previous version reviewed by:  **Heads of IT**  **JUCD Cyber Security Group**  Derbyshire Digital and Data Board |
| **Approved by** | Derbyshire Digital and Data Delivery Board |
| **Approved date** | 28th November 2023 |
| **Date for next review** | 28th November 2024 |
| **Version number** | V1.1 rewrite to reference the published national cyber strategy |

1. **Introduction**

The effective delivery of health and social care is highly dependent on the availability information and the information systems used to deliver care. Over recent years there have been an increasing number of attacks on information and information systems. While some of these have been successful and have resulted in severe disruption to services, many more have been prevented. The threat remains significant and is only expected to grow. It is therefore critical that the owners of information and information systems across Joined Up Care Derbyshire provide the highest levels of cyber security. Effective cyber security will significantly reduce threat and will place Joined Up Care Derbyshire in the best possible position to respond to any successful attack.

The purpose of this document is to set out a strategy which enables us to work collectively across Derbyshire in providing effective cyber security.

1. **What is Cyber Security?**

Cyber security is the practice of ensuring the confidentiality, integrity and availability (CIA) of information.

* Attacks on Confidentiality – stealing, or rather copying personal or sensitive information.
* Attacks on Integrity – seeks to corrupt, damage or destroy information or systems and the people who rely on them.
* Attacks on Availability – denial of services, ransomware, etc.

Cyber security refers to the technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

Cyber security is crucial in ensuring our services are kept up and running. It is also vital in ensuring the public trusts the organisations providing health and social care with their information. A cyber-attack could have very serious consequences, both in terms of disrupting services and through damage to Joined Up Care Derbyshire’s reputation.

1. **Threats**

Threats to the confidentiality, integrity and availability of our information come in a number of forms.

**Cybercriminals**

Cybercriminals are generally working for financial gain, either selling illegally gained information or holding organisations to ransom for the release of data or the protection of reputation.

Key tools and methods used by cybercriminals include:

* + Malware – malicious software such as viruses, that could have an adverse impact on organisations or individuals
  + Ransomware – a kind of malware that locks victims out of their data or systems and only allows access once money is paid
  + Phishing – emails which seek to trick recipients into divulging log in credentials, providing the criminals with access to systems

**Employees**

Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party for financial gain. Additionally, information can be released due to human error or a lack of awareness about the particular risks involved.

**State Sponsored Attackers**

Some hostile foreign intelligence agencies may directly or indirectly, using sponsored groups, target UK organisations and infrastructure. This may be to steal sensitive information or to cause disruption with the aim of undermining confidence in the target state.

**Hacktivists**

Hacktivists may take over public websites or social media accounts to raise the profile of a particular cause. These attacks can disrupt services or cause reputational damage.

**Physical Threats**

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster natural or otherwise that impact IT systems.

1. **Vulnerabilities**

Vulnerabilities are weaknesses in an organisation that a threat actor; such as a hacker, nation-state, disgruntled employee, or other attacker, can exploit to adversely affect data security.

Cyber vulnerabilities may include a subset of those weaknesses and focus on issues in the IT software, hardware, and systems an organisation uses.

* Poor System Maintenance – IT systems should be updated and regularly checked. It is essential that the systems are fully updated and appropriate fixes are applied and that access is appropriately controlled
* Weak Authentication – Passwords, as wells as other forms of authentication such as smartcards or Multi Factor Authentication, an processes must follow best practice to mitigate unauthorised access to systems.
* Aged Software – To ensure that legacy software is eliminated and, where this is not possible, that any risks are mitigated.
* Poor Staff Awareness – It is fundamental that all employees are aware of cyber security and how to support this.

1. **Risks**

Risk is the potential for a vulnerability to be exploited by a threat. Cyber risk management is a fundamental part of the broader risk management to ensure cyber security challenges are fully identified and that appropriate action is carried out

to mitigate the risk.

1. **National Strategic Context**

A small number of key documents set out the context for the delivery of cyber security across and health and care.

**National Strategy for Cyber Security for Health and Care**

NHS England has recently published the National strategy for cyber security for health and care, ‘A cyber resilient health and adult social care system in England: Cyber security strategy to 2030’.

The national strategy is based on ‘Five pillars’, which are designed to support organisations in meeting its vision for a cyber-resilient health and social care sector.

The 5 pillars are:

1. focus on the greatest risks and harms
2. defend as one
3. people and culture
4. build secure for the future
5. exemplary response and recovery

These 5 pillars will be supported by a national implementation plan which will detail activities and define metrics to build and measure resilience over the next 2 to 3 years. The implementation plan will be reviewed nationally every 2 to 3 years to ensure it remains responsive and relevant to the changing challenges.

The national strategy for cyber security for health and care sets out specific requirements for integrated care systems in relation to cyber security and the five pillars outlined above. These requirements are set out in Appendix 1.

**What Good Looks Like**

Chart

Description automatically generatedWhat Good Looks Like (WGLL), produced by NHS England, sets out a specific framework for digital best practice in the NHS. The framework is based on seven success measures shown in the figure adjacent. The ‘Safe Practice’ element describes What Good Looks Like in relation to cyber security.

The WGLL framework contains guidance for both singular NHS Provider Trusts and for Integrated Care Systems and sits alongside the national cyber strategy. The requirements contained within the WGLL framework are set out in Appendix 2.

There is a considerable degree of overlap between the Provider Trust and ICS versions of the Safe Practice requirements. There is also a recognition within the document that the relative immaturity of ICSs means that some of the requirements at the ICS level will require a period of time to develop.

1. **Joined Up Care Derbyshire’s Approach to Cyber Security**

The constituent stakeholders of JUCD will adopt a joined-up approach to cyber security. In developing this approach, we recognise that the constituent organisations within JUCD currently retain different IT infrastructures and challenges. To effectively mitigate threats and provide the best possible cyber security posture across JUCD will require a mixture of local organisational and JUCD-wide action.

As the maturity of the ICS grows, we will look to develop our co-ordinated approach across Derbyshire in line with the requirements placed on ICSs. This approach will enable organisations to move quickly to improve their position and address any gaps. At the same time, we will exploit opportunities for joint working and ensure that any local developments are shared and considered within the wider strategy. As JUCD matures, we will shift from organisational centric actions to more JUCD-wide actions.

Our strategic approach to cyber security will be aligned with the national strategy for cyber security for health and care, ‘A cyber resilient health and adult social care system in England: Cyber security strategy to 2030’ and will be framed by the wider JUCD Digital and Data Strategy.

The JUCD approach to cyber security will primarily draw on the national cyber strategy to guide our approach and actions.

1. **Delivery**

The strategy will be progressed through an action plan which will in turn, reflect the iterations of the national strategy implementation plan, produced as part of the national strategy. In advance of those national implementation plans, the JUCD delivery plan will be based on the ICS requirements outlined in the national strategy.

In addition to the overarching requirements set out in national strategy, the JUCD action plan will be informed by a number of other contributing factors. These will include other emerging national requirements from outside of the published strategy, national risks, and emerging local risks.

1. **Oversight**

The effectiveness of our strategy must be underpinned by collaboration and communication between organisations within the JUCD family. We will ensure that a forum is in place to share our cyber security information from risks to responses. The JUCD Cyber Security Group, comprising of senior information technology staff and cyber security specialists, will seek to deliver the strategy outlined above and be the specialist point of reference for cyber security across Derbyshire.

The JUCD Cyber Security Group will report to the JUCD Design Authority and through that group, to the Derbyshire Digital and Data Board.

**Appendix 1**

**ICS Requirements - A cyber resilient health and adult social care system in England: Cyber security strategy to 2030**

**Pillar 1: focus on the greatest risks and harms**

ICSs will:

* identify and record risks within their ICS, including supplier cyber risks, that would affect the local system’s ability to function
* engage with a plan at ICS level to mitigate risks, invest and review progress
* ensure cyber risk is reviewed as part of broader corporate risk management
* ensure providers maintain an understanding of their suppliers’ cyber security controls and risks

**Pillar 2: defend as one**

ICSs will:

* create an ICS-wide cyber security strategy to drive security across the system
* allocate funding to deliver the strategy, establishing governance to review and align plans and ensuring member and wider partner involvement
* align with agreed cyber security standards when using existing and new cross-organisational systems

**Pillar 3: people and culture**

ICSs will:

* develop an appropriately resourced and accountable cyber security function to manage cyber risk
* develop strategies to recruit and maintain an adequate cyber support function through a combination of ICS and organisation resource
* embed cyber security decisions into multi-disciplinary forums across the ICS to ensure a holistic cyber security culture with the support of the ICP
* encourage collaboration across organisations to share good practice and address deficiencies, supported by the ICP highlighting where coordination is needed and holding partners to account on delivering key priorities
* lead by example in implementing a ‘just culture’ at ICS level in approaching any identified cyber vulnerabilities

**Pillar 4: build secure for the future**

ICSs will:

* build systems and services cyber secure by design, including engaging suppliers on their cyber security in alignment with national engagement
* regularly engage organisations on compliance with standards and frameworks
* develop a cyber security programme underpinning the objectives of the strategy and outline milestones and metrics

**Pillar 5: exemplary response and recovery**

ICSs will:

* outline responsibilities and expectations of member organisations for response and recovery, as well as for a central accountable function
* ensure the ICS and all members have a rehearsed plan for responding to, managing system downtime during, and recovering from a cyber attack
* engage with and understand outcomes from dry-run exercising and post-incident reviews, identifying and responding to common themes for their ICS
* lead on ICS-wide incident response ‘dry run’ exercising
* develop central ICS resilience with the impact of loss or unavailability of critical ICS-wide systems understood and mitigations agreed

**Appendix 2**

**What Good Looks Like – Safe Practice**

Provider Success measure 3 - Safe practice

What does good look like?

Organisations maintain standards for safe care. They routinely review digital and data systems to ensure they are safe, robust, secure, sustainable and resilient. Digitally-enabled outcome-driven transformation is at the heart of safe care.

Your organisation would:

* comply with the requirements in the Data Security and Protection Toolkit which incorporates the Cyber Essentials Framework
* fully use national cyber services provided by NHS Digital
* have a secure and well-tested back-up, a plan to get off and stay off unsupported systems, and a rapid turn-around of High Severity Alerts
* establish a process for managing cyber risk with a cyber improvement strategy, investment and progress regularly reviewed at board level
* have an adequately resourced cyber security function, including a senior information risk owner and data protection officer (DPO)
* have an adequately resourced clinical safety function, including a named CSO, to oversee digital and data development and deployment across all care services
* establish a clear process for reviewing and responding to relevant safety recommendations and alerts, including those from NHS Digital (cyber), NHS England and NHS Improvement, the Medicines and Healthcare Products Regulatory Agency (MHRA) and the Healthcare Service Investigation Branch (HSIB)
* ensure clinical systems and tools meet clinical safety standards as set out by the Digital Technology and Assessment Criteria (DTAC) and DCB0129 and DCB0160
* ensure you are compliant with NHS national contract provisions related to technology-enabled delivery (for example, clinical correspondence and electronic discharge summaries)

What Good Looks Like, NHS England, 2021

ICS Success measure 3 - Safe practice

What does good look like?

Organisations across the ICS maintain standards for safe care, as set out by the Digital Technology Assessment Criteria for health and social care (DTAC). They routinely review system-wide security, sustainability and resilience.

Your ICS would:

* have a system-wide plan for maintaining robust cyber security, including development of centralised capabilities to provide support across all organisations
* establish a process for managing the cyber risk with mitigation plans, investment and progress regularly reviewed at ICS level
* have an adequately resourced ICS-level cyber security function, including a senior information risk owner and data protection officer (DPO)
* ensure that you fully use national cyber services provided by NHS Digital
* ensure the organisations in your ICS are supported to comply with the requirements in the Data Security and Protection Toolkit which incorporates the Cyber Essentials Framework
* have an adequately resourced clinical safety function, including a named CSO, to oversee ICS-wide digital and data development and deployment
* ensure ICS-wide clinical systems meet clinical safety standards as set out by DTAC and DCB0129 and DCB0160
* establish a clear system-wide process for reviewing and responding to relevant safety recommendations and alerts, including those from NHS Digital (cyber), NHS England, the MHRA and the Healthcare Service Investigation Branch (HSIB)
* ensure compliance with NHS national contract provisions related to technology-enabled delivery, for example, clinical correspondence and electronic discharge summaries