



Bath and North East Somerset,
Swindon and Wiltshire Together

Bath and North East Somerset, Swindon and Wiltshire Integrated Care System

Our Cyber Strategy Summary 2025-2030

Defend as One to become the most cyber secure ICS in the country

TLP:CLEAR



Disclosure is not limited

Please note this is a public summary of the ICS cyber strategy, the content has been significantly simplified, and full details of ICS cyber security systems and improvement have been removed.

The full version is TPL: Amber Strict Limited disclosure, restricted to participants' organization.

FINAL Board Approved November 2025



Section 1

Summary

The Bath and North East Somerset, Swindon and Wiltshire (BSW) Integrated Care System (ICS) Cyber Strategy 2025–2030 sets out a unified, collaborative, and risk-based approach to cyber security across the region’s health and care system. With the vision to “**Defend as One to become the most cyber secure ICS in the country,**” this strategy aligns with national priorities and responds to the growing complexity and severity of cyber threats.

Strategic Context

Healthcare is increasingly reliant on digital infrastructure, making cyber resilience essential to patient safety and service continuity. The strategy responds to rising national threat levels, regulatory changes, and the need for consistent measurable cyber maturity metrics across partners to ensure we focus on getting the basics right.

Key Strategic Priorities

- **System-wide collaboration** through shared tools, policies, playbooks, and governance.
- **Adoption of national services** making full use of current and future national NHS cyber services.
- **Standardised cyber risk management** and performance tracking via a unified ICS cyber score.
- **Investment in workforce development** through apprenticeships and training.
- **Annual cyber exercises** to test and improve incident response across the ICS

Strategic Objectives

- Aligned standardised deployment of **logging and privilege access management solutions** by April 2026.
- Implementation of **standardised security baselines** for all devices.
- Aligned standardised **use of antivirus and endpoint protection**.
- Engagement with the **NHS Cyber Security Apprenticeship Scheme**.
- Continued development of the **Cyber Cell** for incident coordination.

Due to NHS England’s scope only NHS organisations and GP primary care are in scope for centrally funded national cyber services. This strategy intent remains applicable to wider system partners where the strategy objectives do not include the adoption of national cyber services or solely rely on NHS funding streams. As a result BSW NHS orgs will be asked to approve this strategy where other partners will be asked to note and create alignment in applicable areas.

External Drivers

- Hostile cyber-attacks are a Tier 1 national risk.
- Ransomware and supply chain attacks remain prevalent.
- Regulatory shifts, including the DSPT alignment with the Cyber Assessment Framework (CAF), require proactive compliance.
- Move for analogue to digital growing the number of digital systems

Delivery and Governance

The strategy is governed by the BSW Digital Board, Technical Design Authority (TDA), and Cyber TDA, with delivery milestones set through to 2027. Success will be measured through improved cyber scores, reduced risk exposure, and enhanced system-wide resilience.



Section 2

Context

Healthcare is more than ever, dependent on digital solutions for the prompt, safe and effective delivery of data and information to those that need it, this will only increase in the future as we become more reliant on digital technologies.

Cyber incidents remain a real and present risk to business functions, organisational objectives, and patient safety.

Confidentiality, Availability and Integrity of the data that we process and store on behalf of our patients and that is required for operational functions is fundamental. There are legal, regulatory, and ethical obligations that ICS member organisations must fulfil

Our strategy outlines how the ICB will bring together the ICS member organisations to collaboratively deliver long term cyber security direction and objectives. Our strategy outlines objectives and how they are aligned to the five pillars in the Cyber security strategy for health and social care: 2023 to 2030

[Cyber security strategy for health and adult social care to 2030 - NHS England Digital](#)

All recommendations in this strategy are based upon key principles firmly grounded to the overarching ICS principle to **“work together”** and **“defend as one”**.

Each initiative within our strategy will link back to the 5 pillars

5 pillars of Cyber security strategy for health and adult social care to 2030

🚫 Focus on greatest risks and harms

Understand risks
Increased visibility
Proportionate mitigations
Network and Information Systems (NIS) regulations are understood and used

✳️ Defend as one ← **Key overarching BSW ICS Cyber Principle**

Collaborative working
Coordinated threat intelligence
Clear accountability
Services fully used

👥 People and culture

Cyber security as a profession
Diverse cyber workforce
A 'just culture' of fairness, openness and learning
Everyone understands their role

🛡️ Build secure for the future

Emerging risks understood
Critical supply chain engaged
Secure by design
Clear and aligned standards

🚨 Exemplary response and recovery

Minimise the impact of a cyber-attack on patient and service user care



Section 3

Strategic Vision

Vision

“Defend as One to become the most cyber secure ICS in the country”

The BSW’s cyber security sets out to make our ICS a cyber resilient healthcare system by implementing cost-effective, collaborative, agile, risk-based and intelligence-led security capabilities, prioritising making best use of national and regional solutions.

We will deliver this by taking a joined-up ICS wide approach to cyber doing things once across the ICS where practical to **‘defend as one’**

Where national toolsets are not available and the need for additional IT / Cyber toolsets are required, the ICS will collectively agree the toolset approach to be adopted, to ensure the **‘defend as one’** approach is achieved. Where existing toolsets exist today, the future approach will be to move to a unified toolset approach and delivery model



BSW Cyber Strategy

Agreed Principles: All cyber initiatives created as a result of this strategy should be tested against the key agreed principles shown below, this is critical to ensure a single vision and approach. Schemes that do not align with these principles should not take place.



- **ICS Collaboration**
- **Common cyber toolsets with standard ICS processes and policies**
- **Making full use of national tools over other solutions. Mature the use of common tools we already have**
- **Consistent ICS Cyber Risk Management and board reporting.**
- **Growing our own cyber talent**
- **Building on our Cyber Cell for incidence response**
- **Further links with Local Authorities and other non-NHS local providers with robust contracts**
- **Targeted realistic and achievable**
- **Alignment to the national Data Security Protection Toolkit**

Please not this is a public summary of the ICS cyber strategy, the content has been significantly simplified, and full details of ICS cyber security schemes and improvement have been removed.

The full version is TPL: Amber Strict Limited disclosure, restricted to participants’ organization.