Freedom of Information Request: Our Reference CTMUHB_421_25

Thank you for your request for information received on the 08 September 2025, regarding cybersecurity standards. Please find the response from Cwm Taf Morgannwg University Health Board set out below:

You asked:

1. **Current Certifications**

   Please disclose which national or international cybersecurity standards the organisation currently holds a formal certification for. This should include, but is not limited to, standards such as Cyber Essentials (CE), Cyber Essentials Plus (CE+), IASME Level 1 & 2, and ISO/IEC 27001.

   We can confirm that Cwm Taf Morgannwg University Health Board (CTMUHB) does not hold any certification for cyber security. Whilst schemes such as CE+ and NIST are achievable for some organisations, the scale and scope of the NHS Wales network make this prohibitive. CTMUHB has its own Cyber Improvement plan and used CE+, NIST, CIS and other relevant schemes as informative references.

2. **Welsh Government Directives**

   Kindly specify any national or international cybersecurity standards for which the Welsh Government has formally mandated or requested certification from your organisation. This pertains to recorded communications, contracts, or policies where such a directive is explicitly stated.

   As an Operator of Essential Services (OES), CTMUHB aligns to the Network and Information Systems (NIS) Cyber Assessment Framework (CAF), and report to Welsh Government via the NHS Wales Cyber Resilience Unit (CRU).

   The Network and Information Systems Regulations 2018: guidance to the health sector in Wales [HTML] | GOV.WALES

3. **Historical Certifications**

   Provide details of any national or international cybersecurity standards to which the organisation was previously certified, but for which the certification has since lapsed or expired. For each expired certification, please include the corresponding expiry date.

   Same as answer for Current (please see response to Q1).

4. **In-Progress Certifications**

   Please detail any national or international cybersecurity standards for which the organisation is currently undertaking the certification process.

   None.

5. **Assessment Outcomes**

   Disclose whether the organisation has failed any formal assessments for national or international cybersecurity standards. If a failure has occurred, please provide the name of the standard and the date of the failed assessment.

   The NIS Cyber Assessment Framework (CAF), as applied within NHS Wales and aligned with the National Cyber Security Centre (NCSC) guidance, assesses organisations against four high-level objectives:

   Objective A – Managing Security Risk

   Objective B – Protecting Against Cyber Attack

   Objective C – Minimising the Impact of Cyber Security Incidents

   Objective D – Detecting Cyber Security Events

   These objectives are further broken down into 14 principles and 39 contributing outcomes, each supported by detailed Indicators of Good Practice (IGPs)

   CTMUHB has assessed critical systems against this criteria. Outcomes are varied depending on the system and its architecture/design. Any systems that don’t meet the standards form part of a risk and action plan for remediation.