



Water for the North West

United Utilities Water Limited

Haweswater House
Lingley Mere Business Park
Lingley Green Avenue
Great Sankey
Warrington WA5 3LP

Telephone: 01925 237000

unitedutilities.com

Baroness Lloyd of Effra
Parliamentary Under Secretary of State
Department for Science, Innovation & Technology
70 Whitehall
London
SW1A 2AS

14 May 2026

By email

Dear Baroness Lloyd,

Many thanks for your letter dated 22 April 2026 inviting United Utilities to sign the government's Cyber Resilience Pledge. At a time of heightened global cyber threat activity, we strongly welcome this initiative and wholeheartedly support the government's commitment to strengthening the UK's cyber resilience.

United Utilities takes cyber security extremely seriously and has established a mature, industry-leading cyber resilience programme, underpinned by a strong security-first culture across our organisation. The actions required under the pledge closely align with our existing cyber strategy and the pledge provides a valuable framework for demonstrating shared commitment between Government and industry.

Below I have set out how we comply with actions one and two of the pledge and meet the purpose of action three. We would welcome a further discussion with your team on the particulars of action three, to explain how our current supplier arrangements are equivalent to or exceed the Cyber Essentials Certification.

It is also worth noting that beyond our own organisation, United Utilities plays a leading role across the sector, convening the industry cyber security network that brings together cyber leads from across the water industry to share threat intelligence and best practice. We are strong advocates of collaboration and transparency, recognising that collective resilience is essential to protecting essential services and national interests.

Make Cyber a Board responsibility

We strongly support the action that cyber security must be owned at the very highest level of an organisation and cyber resilience has long been embedded as a core board responsibility. We have previously implemented the principles set out in the Cyber Governance Code of Practice and our board training follows the same principles of the National Cyber Security Centre's (NCSC) Cyber Governance Training.

Sign up to Early Warning

We strongly support the action of early threat detection and we have been an active participant in the NCSC Early Warning service since its inception. It is now a core component of our cyber defence strategy and gives us increased confidence in the resilience of our perimeter and critical systems.

Require Cyber Essentials across supply chain

We strongly agree with the principle of establishing a minimum cyber security standard across the supply chain as a cornerstone of organisational and national cyber resilience. We apply this principle at scale across a large, complex and critical supply chain, supporting essential services and national infrastructure.

Our current supply-chain cyber assurance arrangements are rigorous and comprehensive, requiring suppliers to evidence their security posture against one or more recognised and robust cyber security frameworks, allowing us to assess maturity proportionately to risk and criticality. These frameworks include:

- NIST Cyber Security Framework
- NCSC Cyber Assessment Framework (Principles A4.a and A4.b)
- NCSC Cloud Security Principles
- NCSC Early Warning Programme (from January 2026)
- PCI DSS
- Cyber Essentials
- Cyber Essentials Plus
- ISO 27001 / ISO 27002
- SOC 2
- CIS Critical Security Controls

In addition, our suppliers are required to complete a comprehensive assurance questionnaire covering technology, processes, governance, culture and people. This layered approach enables us to assess real-world cyber resilience rather than simple framework compliance and provides stronger assurance across a diverse supplier base.

Obtaining Cyber Essential Certification for medium and large suppliers, with tens of thousands of endpoints and extensive internet-facing infrastructure, would require significant reconfiguration of mature hardware and software management environments to operate on an “always-on” basis. This will increase costs and complexity across the supply chain, which will ultimately be borne by water customers.

While we therefore do not intend to apply Cyber Essentials Certification requirements on a uniform basis to all suppliers, we do believe that our approach delivers equivalent outcomes to the intent behind action three of the pledge.

We support the purpose of the pledge and we would welcome the opportunity to work collaboratively on action three with the intention to sign up to the pledge in the near future. We would be very happy to discuss any questions you may have and Jon Wyatt, our Chief Security Officer, would be delighted to engage and share further detail on our approach.

Yours sincerely,



Louise Beardmore

Chief Executive Officer