Information Security Addendum

This current consolidated Information Security Addendum was published on 1 June 2026.

Kudo is committed to protecting both the organisation's and client information assets against all internal, external, deliberate or accidental threats.

We are committed to establishing, implementing and maintaining an Information Security Policy that is appropriate to the purpose and context of the organisation and supports its strategic direction.

At Kudo, our vision is to make asset operations and site work management safer, easier and more efficient for the renewable energy sector and associated industries. We strive to provide our clients with products and services that meet and even exceed their expectations and are committed to continuous improvement.

Certifications and Independent Assurance

Kudo has established an Information Security Management System (ISMS) that provides a framework for measuring and improving our performance. We are certified to the ISO 27001:2022 standard.

- ISO 27001:2022 — Certificate No. 212041/A/0001/UK/En, issued by United Registrar of Systems (URS), certifying our Information Security Management System. Scope: Design, Development and Support of Software Solutions for Work Management and Health and Safety of Operations.
- ISO 9001:2015 — Certificate No. 212041/B/0001/UK/En, issued by United Registrar of Systems (URS) certifying our Quality Management System.
- Independent Penetration Testing — the KUDO platform undergoes regular independent penetration testing. In September 2025, CREST-certified penetration testing was conducted by NCC Group, one of the UK's leading independent cybersecurity assurance firms, assessing the platform's security and data isolation controls. Penetration testing is conducted on an annual basis as part of our ongoing security assurance programme.

How We Achieve This

We achieve our information security objectives by ensuring:

- Information security objectives are established
- Confidentiality of information is secured against unauthorised access and misuse
- Integrity of information is maintained
- Availability of information and systems is maintained
- Contractual, legal, and regulatory requirements are met
- Business continuity plans are developed, maintained and tested
- Physical, logical, environmental and communications security are maintained
- Information security training is mandatory for all employees
- All actual or suspected information security events or incidents are reported and thoroughly investigated
- Independent security assurance is obtained through certification and regular penetration testing as set out above

Continuous Improvement

To further support this we monitor and review our performance to make sure we are delivering the expected results and that we:

- identify and address any areas where we can improve;
- work in partnership with our clients to understand their goals and better meet their needs;
- champion security as a core value within our company culture;
- support and encourage each other to engage with and take ownership of security through education, coaching and sharing of best practice;
- adopt a “right first time” mentality, taking responsibility for our actions and outcomes;
- lead by example through a strong management commitment to information security and by having clear communication, goals, and support to achieve our objectives; and
- undertake management reviews of performance.

Compliance with this policy is mandatory.

This policy is reviewed every two years (or more frequently if there have been significant changes in the type and nature of our activities, or upon material changes to our certification status) and revised as required to ensure it remains current and appropriate for the business.

Signed: Leanne Ramage

Position: Managing Director

Date: 1st June 2026