Security Policy

L2 Business Consulting Limited (L2) are an UK based independent technical consultancy working in sectors which utilise ionising radiations and/or radioactive substances. Our Customers include investors, plant owners, contractors, consultants, regulators and the supply chain.

L2's security policy outlines our guidelines and provisions to protect sensitive business information and preserving the security of confidential data relating to our interested parties by mitigating cybersecurity risks to our technology infrastructure from unauthorised access.

L2 hold accreditation to the Cyber Essentials Standard.

L2 is fully committed to full compliance with:

The Nuclear Industries Security Regulations 2003 (as amended) which provide the essential foundation for our security disciplines: physical; personnel; transport; and cyber security and information assurance applied across our work within the UK civil nuclear industry. We recognise that strict adherence to these requirements is essential and have captured these requirements in L2 WI/03 – Security Instructions.

It is our policy to:

- *Have effective Personnel Security – only engaging suitably security vetted personnel where required and promoting a culture of high security standards.*
- *Implement appropriate Physical Security – ensuring appropriate physical security of our offices and staff to prevent malicious damage, theft, or misuse of information.*
- *Ensure Information Security of Sensitive Nuclear Information (SNI) – ensuring protection by physical methods, implementation of IT security and ensuring adherence to industry procedures.*
- *Promoting an effective Security Culture and awareness in our business to ensure safe, event free working.*

BS ISO/IEC 27001:2022 Information security management systems standard is used by L2 and enables the organisation to establish an information security management system and apply a risk management process that is adapted to our needs, mitigating the risks of breaches and cybercrime. We recognise that strict adherence to these requirements is essential and have captured the technical controls in L2 WI/03, including:

- *Firewalls to secure the network from cyberattacks, preventing malicious and unwanted content entering our network and unauthorised access such as hackers or insiders.*
- *Secure configuration security measures implemented when we established the L2 computers and network devices to reduce unnecessary cyber vulnerabilities and preventing unauthorised exploitation.*

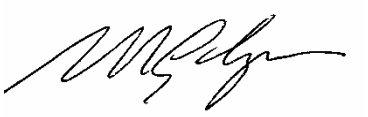
Security Policy

- *Security update management implementing software updates that provide patches or new features to fix existing security flaws or protect against anticipated security problems.*
- *User access control based on employee credentials and then authorizing the appropriate level of access once they are authenticated. Passwords, Pins, Multi-Factor Authentication (MFA) and biometric scans are all credentials commonly used to identify and authenticate L2 users.*
- *Malware protection to ensure cyber security that periodically scans our computers to identify, quarantine, and eliminate any malware keeping our systems secure.*

The Managing Director has overall responsibility for ensuring that our Information Security Policy is integrated into our business plan, strategy, and business processes. The day-to-day management of security is undertaken by the Security Controller (SC).

This Security Policy will be reviewed on an on-going basis by the Board of Directors to ensure that it remains appropriate to our activities.

This Security Policy and the company's IMS shall apply to all activities we undertake. It shall be communicated and apply to all personnel, suppliers, and stakeholders.



MARK LYONS
MANAGING DIRECTOR
Rev: F; September 2025