



Job Description

Title:	Head of Information Security
Hours:	9.30 am to 5.30 pm, but may be required to work overtime. flexible applications considered
Working week:	Monday to Friday
Responsible to:	Chief Information Officer (CIO)
Purpose of job:	The Head of Information Security is responsible for leading and continuously developing Kingsley Napley's cyber security capability ensuring the confidentiality, integrity and availability of the firm's information systems, data and services. Reporting to the CIO, the post holder will be accountable for the delivery of the firm's cyber security strategy, security operations, incident response, security assurance, supplier security and cyber risk management, ensuring activity is clearly prioritised against business risk, client expectations and the firm's strategic objectives. The role will maintain ownership of the firm's ISO27001 Information Security Management System, Cyber Essentials Plus certification and wider security policies and standards. The post holder will work closely with the Chief Legal Officer through a dotted-line reporting relationship, supporting the firm's wider governance, regulatory and client assurance obligations, DPO-related activities, client tenders and regulatory compliance matters. The role will work in close partnership with the Head of IT Operations, Head of Data and key business stakeholders to ensure security is embedded across technology, data, operational and business initiatives. Success in the role will be measured by demonstrable improvements in cyber maturity, effective operation of the SOC, timely remediation of material security risks, successful maintenance of key certifications, clear senior leadership reporting and the consistent embedding of security controls into technology and business change.

Specific duties:

Cyber Security Leadership

- Develop and deliver the firm's cyber security strategy in line with the firm's goals and risk appetite.
- Lead and continuously improve the firm's cyber security capability, roadmap and maturity.
- Act as the firm's senior cyber security subject matter expert.
- Provide security leadership across technology including data, cloud, infrastructure and business projects and initiatives undertaken.
- Promote a positive cyber security culture across the firm.
- Define clear security objectives, success measures and reporting that demonstrate progress against the firm's cyber risk profile and strategic priorities.

Security Operations

- Own and manage the firm's security operations capability.
- Manage and continuously improve the firm's outsourced Security Operations Centre (SOC).
- Oversee security monitoring, threat detection and incident management processes.
- Lead the investigation and response to cyber security incidents.
- Oversee vulnerability management, remediation planning and security improvement activities.
- Coordinate annual penetration testing exercises and remediation programmes.

Security Assurance & Architecture

- Provide security oversight and assurance across infrastructure, cloud platforms, SaaS solutions and business applications.
- Set and maintain security architecture principles and standards that guide technology change across infrastructure, cloud platforms, SaaS solutions, data and business applications.
- Ensure security and privacy-by-design principles are incorporated into technology change initiatives.
- Provide security approval, challenge and assurance at appropriate project governance stages, including early design review, procurement, implementation and go-live readiness.
- Escalate material security risks, exceptions and risk acceptance decisions where proposed solutions do not meet agreed standards or fall outside the firm's risk appetite.
- Work closely with the Head of IT Operations to align operational and security priorities.

Governance, Risk & Compliance

- Maintain responsibility for ISO27001 certification and continuous improvement activities.
- Maintain Cyber Essentials Plus certification.
- Manage security policies, standards and procedures.
- Conduct ongoing security risk assessments and track remediation activities.
- Provide regular reporting to senior leadership.

- Support the CLO and General Counsel on governance, regulatory and compliance matters as required.
- Provide clear, risk-based reporting to the CIO, and senior leadership, including key risks, control effectiveness, remediation progress and areas requiring decision or escalation.

Business Continuity & Resilience

- Support the Chief Legal Officer in maintaining and developing the firm's ISO22301 Business Continuity Management System.
- Coordinate testing and exercising of business continuity and disaster recovery arrangements.
- Support the firm's operational resilience objectives.

Supplier & Client Security

- Own the firm's third-party security assurance programme.
- Assess supplier security controls and support technology procurement activities.
- Support client security audits, due diligence requests and tender responses.
- Provide security input into significant client opportunities and strategic initiatives.

Data Security & AI

- Work closely with the Head of Data, Director of Innovation and CLO/DPO to ensure appropriate security controls are applied to the firm's data, reporting, analytics and AI initiatives.
- Provide security and risk advice relating to AI solutions, data protection and emerging technologies.
- Support the secure adoption of data and AI services across the firm.

Leadership & Team Management

- Lead, develop and mentor members of the Information Security team.
- Manage external security suppliers and partners.
- Establish a culture of accountability, continuous improvement and professional development.
- Support the ongoing development of cyber security awareness and capability across Technology Services.

Every effort has been made to ensure that this is a full description of the tasks and responsibilities of this role. However, it is not an exhaustive list. The job description may be changed or developed at any time to reflect changes as required. However, changes will not be made without full consultation with the post-holder.

Kingsley Napley are committed to creating a diverse environment and is proud to be an equal opportunity employer. All qualified applicants will be considered for employment regardless of race, age, disability, gender identity and expression, sexual orientation, gender reassignment, marriage and civil partnership, pregnancy and maternity and religion.

Person Specification

Job Title: Head of Information Security

	<u>Essential</u>
Education/ Qualification:	• CISSP or CISM certified • An ISO 27001 lead auditor accreditation would be an advantage • A Project Management certification (Prince2, etc) would be an advantage
Knowledge and Technical Ability:	• Demonstrates strong information security leadership experience, ideally within a legal, professional services or similarly regulated environment. • Has a proven track record of owning, maintaining and continuously improving ISO27001 certification and associated information security governance. • Strong experience managing outsourced security partners, including SOC services, incident response providers and specialist security suppliers. • Strong understanding of security operations, vulnerability management, threat detection, incident response and remediation planning. • Good understanding of cloud security, Microsoft/Azure environments, infrastructure security, SaaS assurance and security architecture principles. • Able to provide authoritative security input into technology design, procurement, project governance and go-live decision-making. • Experienced in producing clear executive-level risk reporting, including key risks, control effectiveness, remediation progress and decisions required. • Shows a good understanding of the Data Protection Act, UK GDPR, SRA expectations, client confidentiality obligations and other regulatory frameworks relevant to the firm. • Understands the security, data protection and governance risks associated with AI, data platforms and emerging technologies. • Demonstrates excellent leadership and management skills, with the ability to upskill and empower others through clear direction, coaching and role modelling. • Strong awareness of the wider business context and the ability to align security priorities with the firm's strategy, risk appetite and growth plans. • Ability to provide both strategic leadership and practical operational support where required.
Client Care:	• Proven ability to gain credibility at all levels quickly with excellent relationship management skills • Demonstrates strong influencing skills at senior level • Actively listens to understand; questions and challenges ideas appropriately. Conveys ideas, facts and opinions in clear and understandable terms • Responsive and supportive when working with internal stakeholders across all levels • Strong organisational skills and ability to prioritise. Ability to handle multiple tasks simultaneously with excellent attention to detail
Firm Wide Skills:	• All round strong technical understanding of IT systems

	• Able to balance information security requirements with business priorities, recognising the commercial, operational and client impact of decisions. • Has a strong understanding of the importance of client confidentiality, information security and data protection • Promotes the sharing of best practice and knowledge across the firm
Attributes:	• Clear verbal, presentation and written communication skills • Demonstrates a 'completer/ finisher' mindset – hardworking and committed to meeting tasks and deadlines • Acts as a role model for inclusive management and leadership - encourages an open culture of feedback and improvement • Ability to work independently and as part of a team. • Adopts a positive and open 'growth mindset' to change • Ability to demonstrate behaviour in keeping with the Firm's core values of Teamwork and Respect, Integrity and Fairness, Commitment and Understanding

All applicants who are offered permanent or long term employment, or partnership, will be subject to a criminal record check by the Disclosure and Barring Service (DBS) before the appointment is confirmed. Because Kingsley Napley LLP meets the requirements in respect of exempted questions under the Rehabilitation of Offenders Act 1974, a 'basic disclosure' will be sought. This will reveal 'unspent' convictions. A criminal record is not necessarily a bar to employment or partnership; each matter will be considered on its own circumstances and merits.