NOTTINGHAM TRENT UNIVERSITY

Person Specification

Post Title: Chief Information Security Officer (CISO)		**Post No:**
Organisation Unit: Digital Technologies		
Attributes	**Essential**	**Desirable**
Knowledge	Up to date knowledge of key information security technologies; Knowledge of risk management techniques and best practice.	Knowledge and experience with key national and international information security and digital data standards, legislation and guidance relevant to the academic and research sectors Knowledge of data classification techniques.
Skills	Demonstrable high-level strategic thinking and planning skills; Demonstrated ability and experience in establishing, tracking, measuring and weighing information security risk; Demonstrated ability to operate within a secure environment on sensitive data, data request and information security incidents against strict information security policies. Demonstrated ability to build relationships at different levels of the organisation; Able to build personal and organisational brand externally, and to network with relevant organisations and individuals; Excellent presentation skills and the ability to create persuasive and accessible presentations to non-specialist staff at many levels of the organisation; A demonstrable commitment to leadership development of self and others as it relates to this area of professional specialist work;	An understanding of the PRINCE II and the factors that are critical to success of technical and business change. An understanding of IT service management and processes for service excellence.

Experience	Experience as an information security professional – especially in the area of information security strategy, with associated knowledge of governance, policy creation & maintenance, and monitoring and compliance A proven track record of creating and maintaining an information security service and developing, maintaining, implementing and embedding information security policy in a large institution or organisation. Specifically, proven experience in having dealt successfully with information security incidents. A proven track record working within a risk or information security governance structure. Experience advising, managing and protecting strictly confidential data and datasets or other classified data. Experience Implementing and/or maintaining formal best practice information security compliance or certification (e.g. ISO 27001/2, ISF the Standard of Good Practice for Information Security, COBIT) Experience of evaluating, creating, managing and providing information security training.	Experience building and maintaining a strong information security and risk governance structure within a large organisation. Experience of acting as chair of governance committees or boards.
Qualifications	Graduate calibre with degree or equivalent. Formal certification (CISSP, CISM or CRISC) and/or formal training in information security standards and best practice (e.g.: ISO 27001/2, ISF the Standard of Good Practice for	Current member of IISP (the Institute of Information Security Professionals)

	Information Security, COBIT)	
Competencies (where applicable)	Capable of working with and earning the respect of senior customer stakeholders. Able to articulate and agree a clear vision for the information security strategy.	

See also
PS Guidance Notes