MANCHESTER 1824
The University of Manchester

Job Description

Job title:	Head – Security Architecture and Engineering
Grade:	8
Reports to:	Chief Information Security Officer
Responsible for:	The leadership, line management, motivation, technical direction, development, training and mentoring of assigned staff
Office:	Information Security and Identity and Access Management, IT Services
Date:	April 2023

Overall purpose of the job

The Head of Security Architecture and Engineering is a senior member of staff within the Information Security and Identity and Access Management (IS and IDAM) Division, accountable and responsible for delivering robust enterprise-wide architectural and engineering solutions.

They are a key member of the divisional leadership team, providing strategic direction, anticipating challenges, driving performance and building the capability required to ensure the security of new and existing services.

Key responsibilities, accountabilities and duties

The Head of Security Architecture and Engineering will be accountable and responsible for delivering robust enterprise-wide architectural and engineering solutions. They will manage a team of security architects and engineers and have a high degree of autonomy in decision making.

Security architecture, strategy, policies and standards

- Develop and communicate the vision, principles and strategy for security architects and engineers for multiple projects and technologies, ensuring that solutions are “secure by design”.

- Design and review system architectures for a broad range of complex or uncommon requirements to identify security weaknesses and recommend mitigations.

- Design (or significantly influence) the technical design of a system to enforce security properties that have been derived from first principles to meet a complex or uncommon set of requirements.

- Advise on security architecture implications of technological trends when applied to existing systems, such as migration to the cloud. Explain how those technologies change the security approach required.

- Lead projects and programmes with high strategic impact, solving unprecedented issues and problems and setting a strategy that can be used in the long term across the University and its international centres.

- Establish security architecture policies, standards and design patterns for IT Services.
- Review of all IT Services architecture solutions against business requirements and compliance with security architecture policies, standards and patterns.

- Development and maintenance of Baseline Security Architecture Descriptions.

- Development of Target Security Architecture Descriptions in response to new or changed business requirements.

- Influence key organisational and architectural decisions and interact with senior stakeholders across departments and the higher education sector to reach and influence a wide range of people across larger teams and communities.

- Follow a methodical and repeatable approach to reviewing the security of a system architecture and can describe that approach.

- Contribute to new and innovative security architecture guidance for others to re-use.

Technical security design and implementation

- Lead the technical design of systems and services, justifying and communicating all design decisions, and applying research and innovative security architecture solutions to new or existing problems.

- Gather and decipher subtle and meaningful security needs and understand the impact of decisions, balancing requirements and deciding between approaches
- Work with business analysts and technical IT leads to identify opportunities for re-use and/or integration of components from other sources.

- Assessment and quantification of risks associated with design decisions and reporting of security risks into the IT Services governance framework.

- Lead on quality assurance, and act as the point of escalation for Security Architecture and Engineering within IT Services.

- Guidance and authority on the development or modification of IT services with respect to security.

Line management responsibilities, accountabilities and duties

- Manages, supports and guides the work of groups of staff in line with organisational strategy.

- Allocates responsibilities and assigns packages of work to groups of staff. Ensures that work packages are aligned with the particular skills and abilities of teams. Supports teams in the delivery of work packages. Delegates work to individuals and teams, taking full account of skills and capabilities.

- Integrates staff into teams to perform packages of work, taking account of individual and team capabilities. Considers the importance of skill mix within teams and is sensitive towards team dynamics.

- Optimises the performance of people, measuring and reporting on performance against agreed quality and performance criteria. Collects data on the performance of groups of staff. Gives regular feedback to teams and individuals on performance against agreed work.

- Conducts formal appraisals of the performance of team members. Facilitates a dialogue with team members about expectations, progress, performance and development needs. Participates, as appropriate, in formal processes such as compensation negotiations, grievance procedures, and disciplinary procedures.

- Facilitates effective working relationships within and between teams of staff to ensure high levels of cross-team collaboration. Motivates groups of staff and teams towards a high level of performance. Engages with and empowers groups of staff.

- Promotes and communicates the IT Services Practice Charter and University values, ensuring that these are embedded within the team and are used to make value-based decisions. Acts as a role model for groups of staff, setting a standard, acting professionally at all times and working to a professional code of conduct and ethics.

- Advises individuals on career paths and encourages pro-active development of skills and capabilities. Provides coaching and mentoring to support professional development.

- Manages probationary periods, setting out the requirements of the job, monitoring progress (e.g., regular meetings) and reacting to variances from expectations, organising training and development as required within appropriate timescales.

- Manages teams involved in significant transformation projects and/or during times of change, aligning change programmes with staff skills and capabilities. Supports staff, through difficult and challenging change programmes.

IT Services responsibilities, accountabilities and duties

- You will be expected to demonstrate a commitment to the IT Services Practice Charter and the University's values. The University of Manchester values a diverse workforce and welcomes applications from all sections of the community.

- You may from time to time be required to undertake other duties of a similar nature as reasonably required by your line manager.

- Be available to provide leadership for priority incidents when the need arises which could be outside of standard hours.

Person specification

Experience/education/qualification background:	• Broad-ranging technical knowledge covering application, data, technology infrastructure and security domains with associated experience in designing secure solutions using modern digital technologies, tools and techniques. • Significant experience of designing technical and other security controls to address security risks as part of an overall solution architecture including experience of implementing security controls in a predominantly cloud-services environment. • Experience assuring project outputs against architectural designs and assuring 3rd party architectural designs ensuring adherence to agreed policies, standards, and design patterns. • Experience of managing a wide range of internal and external stakeholders to a senior level with the ability to clearly articulate risks and corresponding controls to support decision making. • May have one or more technology specialisms where you are regarded as an expert in how the specialism supports security architecture design (e.g., micro service architectures, identity, etc.) Desirable qualifications: • CISSP, CISM and/or TOGAF

Competency (Professional, technical or behavioural)	Level	Essential	Desirable
Inclusive Leadership: Able to encourage and inspire others to act inclusively, to engage and value the diversity of thought and background within and beyond their teams and practice an inclusive approach.	Expected behaviour	X	
Leadership: Methods, style, and tactics for leading an organisation, such as influencing, negotiating, flexible thinking, communicating, emotional intelligence, leading innovation and change.	Expected behaviour	X	

Infrastructure/system security: The security threats and vulnerabilities that impact and/or emanate from system hardware, software and other infrastructure components, and relevant strategies, controls and activities to prevent, mitigate, detect and resolve security incidents affecting system hardware, software and other infrastructure components.	Expert in	X	
Network data security: Network security and threat mitigation, including physical, electronic, firewalling, encryption, access, and authorisation; protecting data at rest and in transit; defending against viruses and malware; the impact of Big Data; and the integration of robust security controls into enterprise services and policies.	Expert in	X	
Access control systems: Any tool or system which provides security access control (i.e., prevents unauthorised access to systems).	Expert in	X	
Information architecture: Methods, techniques and technologies for ingesting, securing, processing and using data and information within and beyond an organisation.	Expert in	X	
Stakeholder Engagement: Establishing relationships, analysing perspectives and managing stakeholders from a variety of backgrounds and disciplines. Adapting stakeholder engagement style to meet the needs of different audiences. The identification of key business stakeholders and an assessment of their level of power and interests, and their perspectives to inform the way(s) in which they should be considered and managed.	Expert in	X	
Risk Management: Methods and techniques for the assessment and management of business risks, in particular, security risks related to information, systems, and processes owned by the University.	Expert in	X	
Protective Security: Protective security encompasses the combination and multi-layering of appropriate and proportionate Physical, Personnel and Cyber Security measures to help detect and respond to any attack.	Expert in	X	
Threat Understanding: Threat understanding encompasses evidence-based knowledge, including context, about an existing or emerging threat to assets that can be used to inform decisions.	Expert in	X	
Legal and regulatory environment and compliance: Understanding the legal and regulatory environment within which the	Expert in	X	

University operates and ensuring that the University complies with legal and regulatory requirements and standards related to information security.			