Job Description

Job title: Cyber Security Architect

Grade: 8

Reports to: Head – Security Architecture and Engineering

Office: Information Security and Identity and Access Management, IT Services

Date: April 2023

Overall purpose of the job

The Cyber Security Architect is a key member of staff within the Information Security and Identity and Access Management (IS and IDAM) Division, responsible for addressing the University's cyber security and compliance requirements by developing and delivering appropriate technology solutions. The role may be aligned to one or more of the University's Faculties, ensuring that security strategy supports the needs of each Faculty.

Key responsibilities, accountabilities and duties

The Cyber Security Architect advises and enables technical teams to make security decisions. They provide advice and guidance to ensure common tools and patterns are used effectively to deliver secure systems, and they implement proportionate controls to enable business outcomes. The Cyber Security Architect will be required to effectively translate business objectives and risk management strategies into specific security processes enabled by security technologies and services.

Security architecture, strategy, policies and standards

- Design and review system architectures to identify security weaknesses and recommend mitigations.
- Design (or significantly influence) the technical design of a system to enforce security properties, ensuring that solutions are "secure by design".
- 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.
- Draft security policies, standards, procedures and design patterns to be reviewed and approved by the Head of Security Architecture and Engineering and/or the CISO.

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

- Develop and maintain Baseline Security Architecture Descriptions.

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

- Influence key organisational and architectural decisions and interact with senior stakeholders across divisions and departments.

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

Technical security design and implementation

- Develop and maintain security architecture artefacts (e.g., models, templates, standards and procedures) that can be used to leverage security capabilities in projects and operations.

- 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.

- Assess and quantify risks associated with design decisions and report security risks into the IT Services governance framework.

- Lead continuous improvement of security technologies and processes and support efforts to improve the maturity of Security Controls through continuous collaboration with suppliers, partners and other teams (e.g., Security Operations, Infrastructure and Service Management).

Assurance

- Track developments and changes in the business and threat environments to ensure that they're adequately addressed in security strategy plans and architecture artefacts.

- Validate IT infrastructure and other reference architectures for security best practices and recommend changes to enhance security and reduce risks, where applicable.

- Validate security configurations and access to security infrastructure tools, including firewalls, IPSs, WAFs and anti-malware/endpoint protection systems.

- Conduct or facilitate threat modelling of services and applications that tie to the risk and data associated with the service or application.

- Ensure a complete, accurate and valid inventory of all systems, infrastructure and applications that should be logged by the security information and event management (SIEM) or log management tool.

- Support the testing and validation of internal security controls.

- Review security technologies, tools and services, and make recommendations to the broader IS and IDAM Division for their use, based on security, financial and operational considerations.

Technical specialism and professional development

- Keeps in close touch with and takes a leading role in contributing to current developments in enterprise business architecture within the University and external professional networks. Is fluent at articulating best practice and is a recognised authority in enterprise business architecture.

- Maintains knowledge of the enterprise business architecture at the highest level by representing the University at conferences and seminars; meeting and maintaining contact with other professionals involved in business architecture; and through taking an active part in appropriate professional bodies.

- Provides organisational leadership and guidelines to promote the development and exploitation of enterprise business architecture as a discipline within the University. Initiates and authorises release of quality standards and policies relating to enterprise business architecture.

- Facilitates effective working relationships within and between teams of staff. Motivates groups of staff and teams towards a high level of performance. Engages with and empowers groups of staff. 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 proactive development of skills and capabilities. Provides mentoring to support professional development.

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. • 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 (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	
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	Expert in	X	

perspectives to inform the way(s) in which they should be considered and managed.			
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 University operates and ensuring that the University complies with legal and regulatory requirements and standards related to information security.	Expert in	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.	Proficient 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.	Proficient in	X	
Access control systems: Any tool or system which provides security access control (i.e., prevents unauthorised access to systems).	Proficient in	X	