Job Description

Job title: Network Architect

Grade: 8

Reports to: Head –Infrastructure Services

Responsible for: n/a

Office: Technology, IT Services

Date: January 2023

Overall purpose of the job

The division of Technology leads and owns the University's IT infrastructure and platforms and is accountable for a comprehensive approach across all areas of the University and its international centres. The division is comprised of four departments (Infrastructure Services, IT Operations Centre, Platforms and Infrastructure Programmes) and oversight of strategic managed services contacts.

The Network Architect is senior member of staff within the Technology Division, serving the entire University and its international centres. The Network Architect will provide a clear vision and strategic direction for the University's IT network which includes campus, cloud and hybrid data centre.

Key responsibilities, accountabilities and duties

Network strategy and architecture

- Develop and maintain network architecture that enables UoM to develop and implement network solutions and capabilities that are clearly aligned with business, technology and threat drivers.
- Advance the uptake of SD-WAN technology within UoM.
- Develop network strategy plans and roadmaps based on sound enterprise architecture practices.
- Develop and maintain network architecture artifacts (e.g., models, templates, standards and procedures) that can be used to leverage network capabilities in projects and operations.
- Determine baseline network configuration standards for network, cloud and network segmentation.
- Review network and cloud technologies, tools and services, and make recommendations to the broader Technology team for their use, based on security, financial and operational metrics.
- Liaise with other architects and security practitioners to share best practices and insights.
- Liaise with the business continuity management (BC) team to validate security practices for BCM testing and operations when a failover occurs.

Network security planning and management

- Track developments and changes within IT and threat environments to ensure that they are adequately addressed in security strategy plans and architecture artifacts.
- Participate in application, infrastructure and cyber projects to provide network-planning advice.
- Draft network standards to be reviewed and approved by executive management.
- 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 networks that should be logged by the security information and event management (SIEM).
- Establish a taxonomy of indicators of compromise (IOCs) and share this detail with other security colleagues, including the security operations centre (SOC), information security managers and analysts, as well as counterparts within the network operations centre (NOC).
- Coordinate with DevOps teams to advocate secure coding practices and to escalate concerns related to poor coding practices to the CISO.
- Validate configurations and access to security infrastructure tools, including firewalls, IPSs and WAFs.
- Review network segmentation to ensure least privilege for network access.
- Liaise with the audit teams to review and evaluate the design and operational effectiveness of network-related controls.
- Support the testing and validation of internal controls, as directed by the CISO, Information Governance Office or compliance and risk functions.

Infrastructure strategy and planning

- Validate IT infrastructure and other reference architectures for network best practices and recommend changes to enhance security, reduce risks and improve service availability.
- Design and implement short- and long-term strategic plans to ensure infrastructure capacity meets existing and future requirements.
- Develop, implement, and maintain policies, procedures, and associated training plans department.
- Participate in the development of IT strategies in collaboration with the executive team.
- Conduct research and make recommendations on products, services, protocols, and standards in support of all infrastructure procurement and development efforts.
- Establish service level agreements with other areas.

Acquisition and deployment

- Prepare RFPs, bid proposals, contracts, scope of work reports, and other documentation for infrastructure projects and associated efforts.
- Negotiate with vendors, outsourcers, and contractors to secure infrastructure-specific products and services.
- Assist with the planning and deployment of network measures.

Operational management

- Manage and set priorities for the design, maintenance, development, and evaluation of all infrastructure systems, including LANs, WANs, Internet, intranet, security, wireless implementations, and so on.

- Conduct feasibility studies for various upgrade projects, improvements, and other conversions.
- Define network, hybrid cloud and standards in conjunction with owners and stakeholders.
- Test network performance and provide network performance statistics and reports; develop strategies for maintaining server infrastructure.
- Practice IT asset management, including maintenance of component inventory and related documentation.

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.

Person specification

Experience/education/qualification background:	• Proven record of developing network strategies, based on industry standard architectural principles, for a varied and geographically-diverse infrastructure. • Evidence of applying standards, practices, codes and assessments relevant to IT networks, infrastructure and security. • Experience of network supplier management, from supplier selection through procurement to development and on-going operation. Desirable qualifications: • SABSA, Zachman and/or TOGAF

Competency (Professional, technical or behavioural)	Level	Essential	Desirable
Operational/Service Architecture: Knowledge of the IT/IS infrastructure and the IT applications and service processes used within own organisation, including those associated with sustainability and efficiency.	Expert in	X	
Network traffic analysis: Methods and techniques for the capture of traffic information (packet level) and the forensic analysis of this information into its constituent elements.	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;	Expert in	X	

the impact of Big Data; and the integration of robust security controls into enterprise services and policies.			
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	
Access control systems: Any tool or system which provides security access control (i.e. prevents unauthorised access to systems).	Expert in	X	
Business proposals: Methods and techniques for preparing and presenting business cases, requests for proposal (RFP) invitations to tender (ITT) and statements of requirements/work both verbally and in writing.	Proficient in	X	
Cloud/virtualisation: The principles and application of cloud/ virtualisation (including ownership, responsibilities and security implications). Use of tools and systems to manage virtualised environments.	Proficient in	X	