ROLE PROFILE			
Job Title:	Technical Security Manager	**Job Code:**	CS/I1
Department:	ICT Services	**Version:**	1.0
Reports To:	Head of ICT Services	**Date Created:**	July 2020
No. of direct reports:	0	**Member of:**	ICT Services
No of employees in function:	25	**Grade:**	L
		Budget:	n/a

Is this a politically restricted Post?	~~Yes~~/ No	*(*if yes, see our policy on what this means)*

ORGANISATIONAL CONTEXT

Our Vision as an organisation is:

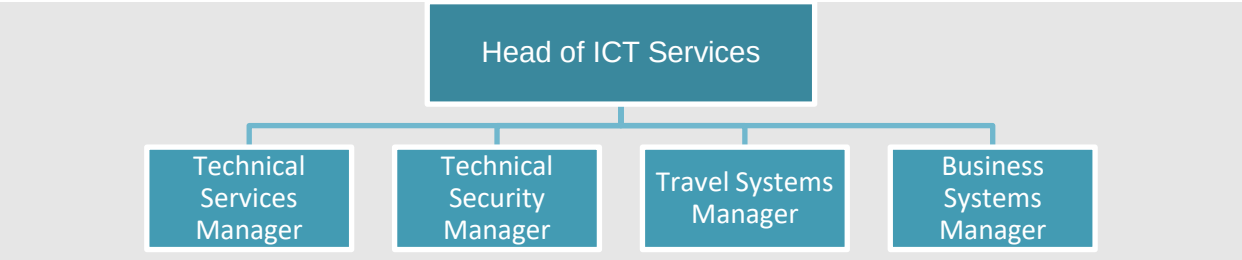
To be a globally recognised economy where good growth delivers high levels of prosperity, jobs and quality of life for everyone.

To achieve this we will:

Secure the means to deliver projects and services needed for growth in the Leeds City Region (LCR), be its voice nationally and internationally, and build the partnerships to ensure the best economic outcomes.

Our department contributes to this by:

Delivering programmes and projects to realise value in order to maximise growth.



Job Overview:

- Lead on the development, technical implementation and enforcement of information security policies including ownership and maintenance of the cyber security emergency response procedures.
- Provide regular evidence that the organisation's technical and service arrangements are appropriately configured to best protect the organisations from cyber-attack and information loss.
- Maintain and develop a proven, acceptable level of security across the Combined Authority's systems.
- Be the technical security lead on high profile projects and daily operations.
- Support the delivery of the organisation's Corporate Technology Strategy, with a particular focus on Cyber Security and Disaster Recovery.
- Manage the external network to ensure robust monitoring and threat protection to minimise any potential for malware attack.

© Design, implement and maintain the systems required for delivery the objectives of your function to support the Combined Authority in achieving its vision.

© Take a pro-active corporate role in the management of your function including participation and delivery of your directorate's objectives.
© Responsible for demonstrating commitment to corporate processes and ensuring that these are delivered at all times.
© Be a visible and enthusiastic manager, encouraging partnership working across the organisation.
© Take a positive approach to self-development.

CRITICAL SUCCESS FACTORS

We break each job down to explain the critical areas for success, ranked by importance.
These indicate the end result or outputs for which the role holder is responsible.

People Contacts:

- Build mutual respect and trust with internal and external stakeholders, working closely with staff and suppliers to ensure the successful delivery of the requirements of all services and the strategic objectives of the Combined Authority, in a safe and secure manner.
- Develop productive cross organisation relationships to further the duties of the role.
- Train staff in ICT Services and Information Governance in the use of security technologies including Microsoft 365 Security Center, Microsoft 365 Compliance Center and Azure security.

© Support partnership working across the organisation and externally.
© Work together with your team to ensure targets are achieved.
© Be an advocate of our strong performance management culture, taking accountability for delivering results.
© Contribute to a positive working environment for your team, with a solid ethic of working towards achievement of our vision.
© Take a proactive approach to internal processes, contributing during meetings and interviews.
© Utilise effective communication channels when working with others.

Technical Duties:

- Establish and maintain appropriate information security standards, policies and controls aligned to ISO 27001, Cyber Essentials and National Cyber Security Centre recommended best practice.
- Management of Microsoft 365 Security Center, Microsoft 365 Compliance Center and Azure security.
- Technically support and develop disaster recovery and capabilities to ISO 27031 standards.
- Conduct regular reviews and manage penetration tests to challenge systems, identify vulnerabilities and perform remedial actions to mitigate identified risks.
- Ensure that all operating system and application patching policies are appropriately applied and are fit for purpose, and any issues are speedily addressed.
- Design and implement an information security management system to operate in a consistent manner across the organisation.
- Lead on or take a senior role in a range of projects, which may include but is not limited to penetration testing, load testing, security awareness, technical policy developments, Azure configuration, disaster recovery, data platform implementation, CRM development, ICT procurements, service management and digitising services.
- Lead on investigations into security incidents within ICT Services and advise on risk and the implementation of remedial actions.
- Provision of regular security reporting to highlight any non-compliance issues and threat analysis.
- Active membership of the organisation's Technical Design Authority and ICT Management Team.
- Responsible for the procurement, appointment and management of technical and commercial security consultants, suppliers and contractors.
- Liaison with internal and external stakeholders, representing the Combined Authority in specialist local, regional and national cyber security discussions.
- Responsible for keeping abreast of current and emerging security and recovery risks.

© Typically works on horizons of one year, in line with the objectives set in the business plan.
© Ensure you have the right procedures in place to achieve your strategic objectives, developing and amending processes as required.
© Forward plan your workload, identifying appropriate solutions and acting accordingly.
© Lead by example on health & safety matters, ensuring compliance with the Combined Authority's health and safety policy.

Financial:

- Responsible for ensuring compliance of third parties to agreed contracts.

© Fulfil the requirements of a budget holder, as detailed in the Corporate Standing Orders and the Financial Regulations.
© Deliver financial results against corporate Key Performance Indicators.
© Analyse and appraise financial related information ensuring financial process deadlines are met.

Impact & Influence:

- Have organisation wide visible responsibility for information and system technical security matters.
- Strong and successful ongoing collaboration with the Information Governance team.
- Lead and motivate multidisciplinary teams for delivery of technical projects and project objectives.
- Be the expert for the management of technical security and improvement activity across the Combined Authority, communicating as an authoritative subject matter expert across all directorates
- Responsible for using strong influencing and conflict resolution methodology, and building relationships with suppliers, to achieve optimum results.
- Ability to analyse and interpret data/information and communicate to a range of audiences using a range of media.
- Attend and provide reports, when required, to the Combined Authority's boards and committees
- Bring others on side to develop a collegiate and consistent approach to organisation wide security and technical resilience.

© Represent the interests of your function within the context of the wider aims of the Combined Authority both internally and externally.
© Foster good working relations across the organisation, building effective departmental relationships.
© Use strong communication skills to influence key customers and stakeholders supporting your function's ability to deliver results in line with the vision.
© Identify and find solutions to communication challenges observed within the organisation.

The above lists of accountabilities are not exhaustive. The role holder will be required to undertake such tasks as may reasonably be expected commensurate with the scope and grading of the role.

THE PERSON

To be fully successful in the role, we believe the following knowledge, skills and experience are required. When recruiting, we are looking for the best candidate match to this, however we know that there are some elements that can be trained and this will be taken into account during the recruitment process.

Knowledge:

© Holds a degree in a relevant field or relevant demonstrable practical experience.
© Information Security qualification such as CISSP, CISA, CISM, or MSc Information Security alongside significant knowledge and experience of IT security systems across multiple technical platforms.
© Practical experience of successfully performing in a similar role with a detailed understanding of major corporate technology systems.

- In-depth knowledge of IT security products, systems and applying security best practice.
- Technical experience of Microsoft 365 and Azure security.
- Demonstrable strong working knowledge of security standards and methodologies such as ISO27001, COBIT, and ITIL and an understanding of relevant data protection legislation.
- In depth knowledge of the current threat landscape in terms of Information and Cyber Security.
- Experience of a broad range of ICT technologies including networking, hardware & infrastructure, operating systems and enterprise voice systems.

People:

© Experience of effectively contributing to department objectives.
© Experience of successfully identifying appropriate communication channels to deliver information.
© Experience of effectively contributing to organisational vision.

- Demonstrable experience of leading multi-disciplinary project teams to deliver a range of complex or high profile security and other technical projects.
- Ability to provide easily understood technical requirements to staff and external partners.
- Able to work in matrix teams that may have physically remote team members, ensuring that others understand the technical issues and requirements.

Technical:

© Demonstrable experience of managing and championing change successfully.
© Strong communication skills with the proven ability to influence, negotiate and challenge.
© Experience of making compelling business cases/ reports to a range of audiences.

- Logical with an excellent grasp of technologies and current risks which organisations must address to build strong, resilient systems that protects data, systems and the wider organisation.
- Ability to demonstrate creative thinking and clear technical leadership in order to deliver agreed business outcomes and lead stakeholders through all stages of delivering complex ICT projects.
- Experience of working in partnership with stakeholders including suppliers, internal owners of key systems who are mostly non-technical people, public and private organisations.
- Ability to evaluate and develop new processes to deliver change management.
- Ability to develop and share best practice and lessons learned across the Combined Authority and externally as appropriate.

Financial:

© Demonstrable experience of successfully managing budgets.

- Knowledge and experience of applying financial systems and procedures for reporting in compliance with internal governance and assurance procedures and requirements of external funders.
- Ability to ensure value for money is obtained through rigorous project appraisal and applied knowledge of competitive procurement and value engineering techniques.

Impact & Influence:

© Proven experience of confidently and professionally conveying information both written and oral in a clear, concise and persuasive style.
© Comprehensive experience of leading, negotiating and influencing stakeholders.
© Experienced in forming and developing effective senior level working relationships with Members, Government and partner organisations to achieve the best outcomes for the organisation.
© Comprehensive experience of providing leadership in a complex public-private sector partnership context.

- Significant subject matter expertise for the management of technical security with the ability to effect improvement activity
- Ability to communicate complex information effectively, accurately and appropriately to different audiences using a range of media.
- Able to negotiate with suppliers and Delivery Partners in the public and private sector and effectively manage conflict resolution.

OUR VALUES & BEHAVIOURS

Championing Our Region | Working Intelligently |Easy to Do Business With | Positive About Change | Working Together

These are our values. We shaped them together and we're proud of them.

We also created a set of behaviours for each of our values. Our behaviours provide us with a way of working and they are our minimum expectations of everyone here.